Federal Aviation
Administration

Information Technology Strategy

Fiscal Years 2006-2008

September 30, 2005

"Envisioning, communicating and achieving the technological future of the Federal Aviation Administration!"

Signature Pages for CIO Council Members

I have reviewed and will support the Corporate IT Strategy that is provided in Sections I – V of this document and the IT Sub-Strategy for my Line of Business/Staff Office provided in Section VI. I will ensure that my Executive approves this document.

Approved by:

________________________________ __________________________
Ernesto Villacarlos (ARP) Date

________________________________ __________________________
Dennis Filler (ATO) Date

________________________________ __________________________
Paul Dykeman (AEP) Date

________________________________ __________________________
Tina Amereihn (AVS) Date

________________________________ __________________________
Phyllis Preston (AOC) Date

________________________________ __________________________
Mark Bruno (ABA) Date

________________________________ __________________________
Rodney Herron (AHR) Date

Craig Lindsay (API) Date

Cindy Cassil (ARC) Date

________________________________ ________________________

Bruce Herron (ASH) Date

Approval Information

Focal Point:	Robert Rovinsky (AIO)
Phone Number:	(202) 493-4019
Submission Date:	September 30, 2005
Revision Date:	NA

Signature Pages for FAA Key Officials

Executive Sponsor

________________________________ ________________________

Daniel J. Mehan (AIO) Date

I support the Corporate IT Strategy that is contained in Sections I – V of this document and the IT Sub-Strategy for my Line of Business/Staff Office provided in Section VI. The contents of both documents will be reflected in my Business Plans for FY2006 – FY2008.

Approved by:

________________________________ __________________________

Woodie Woodward (ARP) Date

________________________________ __________________________

Russell G. Chew (ATO) Date

________________________________ __________________________

Sharon L. Pinkerton (AEP) Date

________________________________ __________________________

Nicholas A. Sabatini (AVS) Date

________________________________ __________________________

Greg Martin (AOC) Date

________________________________   _________________________
Ramesh K. Punwani (ABA)   Date

________________________________   _________________________
Ventris C. Gibson (AHR)   Date

________________________________   _________________________
Paul Feldman (API)   Date

________________________________   _________________________
Ruth Leverenz (ARC)   Date

________________________________   _________________________
Lynne A. Osmus (ASH)   Date

Revision History

Version	Date	Comments
Draft Version 1.0	August 12, 2005	N/A
Draft Version 1.1	August 15, 2005	Added AEP, API, AOC, AGC, and ASH to Section VI
Draft Version 1.2	August 23, 2005	Added input from members of CIO Council and AIO
Draft Version 1.3	September xx, 2005	Added comments from FAA IT Community
Draft Version 1.4	September 9, 2005	Added final comments from FAA IT Community
Final Version 1.0	September 30, 2005	Added LOB/SO IT plans and final comments from IT Community

Federal Aviation Administration

TABLE OF CONTENTS

Federal Aviation Administration

Executive Summary

Information, and the information technology (IT) products and services that create, store and transmit information, are critical to the operation and mission of the FAA. Next to people, the FAA spends more on IT than any other resource. The FAA's Chief Information Officer (CIO), together with the Chief Information Officers' Council composed of the IT leaders and CIOs of the organizations within the FAA that are major users of IT services and technology, produce every three years an IT strategy to guide the future direction of IT within FAA and ensure that it is aligned with the business needs of the agency.

This corporate IT strategy updates the IT strategy for FY 03-05. It builds on the many achievements of the past three years and sets as its "north star" the positioning of the FAA as a leader in three principal areas of government IT by 2008: business value and IT performance; cyber security; and, E-Government. A cornerstone principle of the IT strategy is that to succeed in tomorrow's world of increasing threats, demanding customers, and tight budgets, the FAA must achieve excellence in these three areas; to do less is to risk damaging the agency business needs and mission.

In Business Value, FAA has improved the capability to develop and implement IT systems that support our business needs. Our IT professionals have training in the latest tools and techniques, and program managers for our major programs are becoming certified by the Program Management Institute (or its equivalent). FAA has developed strong and compelling business cases [Exhibit 300s] that have convinced those that fund us to support all of our major IT investments in FY 05, and we have achieved the second highest rating from the Government Accountability Office (GAO) for our IT investment management practices. Good IT program management will help us meet the Flight Plan goals of keeping 90% of our major system acquisition investments on schedule and within 10% of costs by 2009. But this is not enough – in an increasingly competitive environment even air traffic control and safety IT investment must meet the highest standards of government Program management and must achieve top scores from those who rate our investment packages. To be the leader in this area FAA will do the following: Institute best practices in integrated program management, including the full introduction of Earned Value Management throughout the agency; and, achieve similar demonstrated leadership in related areas such as enterprise architecture, process engineering, data management, and cost estimation.

Included in business value is IT Performance. It consists of operating IT as a business resource that can be measured and monitored. The goal builds on several achievements in the past few years, including our major role in the achievement of "green" in E-government by the Department of Transportation, the first cabinet level organization to "get to green" in this area. It builds on the Flight Plan goal to control agency overall costs. The Chief Financial Officer cited IT as the success story in overall agency cost control in FY 05 as the IT community achieved 200% of its targeted savings goal. But FAA must achieve more to be a leader. The CIO for FAA's Air Traffic Organization will reduce costs by consolidating the number and diversity of their IT environments. The CIO for Region and Center Operations (ARC) will measure and improve operations that enable this organization to compete for cross-government administrative services. AIO will work with the FAA IT community to develop a set of key corporate metrics in FY 06 that will define and drive corporate IT services and the CIO Council will achieve excellence in the management and operation of IT against these metrics, again positioning the agency as a leader in the area of IT performance.

In Cyber Security, the agency has built a strong program based on prevention of disruptive attacks and the development of a strong outer defense. Our goal, expressed in the Flight Plan, is to have zero cyber security events that significantly disable or degrade FAA services. We have been successful in meeting this goal. The cyber attacks of the past few years that damaged other federal and private sector organizations did not harm the FAA or interfere with our mission critical applications. The awarding of an A- score in FISMA (the Federal Information Security Management Act) to the Department of Transportation – the first cabinet agency to achieve an A– is a tribute to the efforts of the agency's organizations, as the FAA maintains the vast majority of the department's critical systems. But to maintain leadership and ensure that cyber attacks do not interfere with the operations of the Nations critical air traffic control system or safety systems will not only require maintaining our vigilance, but developing the resilience to isolate and recover quickly from any future successful assault. Thus, we will develop our "android model" defense strategy.

FAA will continue to keep the Department of Transportation "green" in E-government. And, we will coordinate with the Department of Transportation on meeting the deadlines established for a number of Presidential Initiatives. We will focus on reengineering and improving targeted business processes that enable us to build applications that provide services to external customers and promote data sharing across organizational boundaries.

This IT Strategy provides the FAA corporate vision and goals and the project mechanisms to achieve them. We build on the accomplishments of the retiring CIO Dan Mehan and thank the CIO Council for their ongoing commitment, achievements, and cooperation. We also thank the people no longer here, such as deputy CIOs Art Pyster and Greg Dvorak, and our former CIO Council members and colleagues Tim Schmidt and Rick Ford. While stressing the corporate strategies, we recognize the need to have complementary Line of Business and Staff Offices strategies that meet the specific needs of the business units while supporting the overall corporate strategies and have included sections written by each line of business and staff office CIO.

I. Introduction

Background

The Federal Aviation Administration (FAA) is the largest operating administration in the Department of Transportation (DOT) and supports the Department's strategic objectives in safety, mobility, global connectivity, environmental stewardship, and security through *Safer, Simpler, Smarter Transportation Solutions*. FAA makes significant contributions to DOT goals, which are: safety; mobility; global connectivity; environmental stewardship; security (e.g., FISMA); organizational excellence; and, the President's Management Agenda (PMA). In particular, FAA plays a major role in organizational excellence by helping the Department to maintain "green" on the White House Office of Management and Budget (OMB) scorecard for E-government.

Information is critical to the operation and mission of the FAA. Information Technology (IT) drives the creation, processing and delivery of that information in every organization and major business process. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act, was intended, among its many other purposes, to "reform acquisition laws and information technology management of the Federal Government." In Section 5002 of the Act (the "Definitions" section), the Clinger-Cohen Act establishes a three-part definition of information technology as follows:

(A) The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(B) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(C) Notwithstanding subparagraphs (A) and (B), the term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Using this definition of information technology, Agency spending on IT and IT systems accounts for over $3.0 billion annually, the largest cost item after salaries and benefits. The Federal Aviation Administration (FAA) Flight Plan recognizes both the cost and criticality of IT in the Increased Safety, Greater Capacity, and International Leadership and Organization Excellence goals. The FAA IT Strategy Fiscal Years 2006-2008 directly supports these agency goals.

Within the FAA, the Assistant Administrator for Information Services and Chief Information Officer (AIO) has the primary responsibility to formulate agency IT policy and strategy, to protect agency IT assets from cyber-attacks, to ensure alignment between IT investment and agency business needs, and to improve agency business and IT management and operations processes. The current strategy for achieving the mission is to work with key constituents (i.e., the FAA Administrator, Deputy Administrator, Chief of Staff, Chief Operating Officer, Chief Financial Officer, Assistant Administrators, and Associate Administrators) to understand the information technology needs of the agency and team with other organizations to carry out the mission. Accordingly, the goals, strategies, objectives, and outcomes identified in this document reflect not only those of AIO, but include those envisioned by the Agency's Chief Information Officer (CIO) Council, Information Resource Managers, and Information Systems Security Managers (ISSMs). This document also represents a number of IT efforts planned by the various lines of business (LOBs) and staff offices (SOs).

Scope of the FAA IT Strategy Fiscal Years 2006-2008

Previous FAA IT strategies encompassed three separate user community "domains" that consisted of distinct network and system environments, as follows:

- The NAS System Domain includes all information systems and networks that provide critical real-time communication, navigation, surveillance, weather information, flight-planning data, and automation services necessary for safe and efficient Air Traffic Control services, as well as mission support to Departments of Defense (DOD) and Homeland Security.

- The FAA Mission Support System Domain includes all other information systems and networks that provide FAA-specific mission services to the internal and external aviation community stakeholders. Some of the significant services included in this domain are surveillance of airlines and aircraft manufacturers, airmen, aircraft, and medical certification, and the exchange of safety related data with the aviation industry to help anticipate accidents.

- The FAA Administrative System Domain includes information systems and networks that provide for national, regional, and local financial accounting services, agency personnel, payroll, and attendance records, electronic mail, internet, and intranet access, logistical support, and numerous other support functions and activities.

In the course of developing the FAA IT strategy for FY2006 – FY2008, we discovered that these three domains no longer reflect today's user communities. There is strong sentiment around reducing the number of categories to only "two" and replacing the title of "domain" with something more appropriate. Some members of the IT community support the need to define NAS versus Mission Support (including Administrative systems) systems, while other members want to use "Safety" instead of "Mission Support". And, other individuals are leaning towards Safety/Mission versus Corporate/Shared systems. While this issue has not yet been resolved, we plan to agree on a solution in the first quarter of FY06.

For the IT strategy documented herein, we looked at NAS and Non-NAS "resources", in terms of four quadrants (i.e., NAS Applications, Non-NAS Applications, Non-NAS Infrastructure, and NAS Infrastructure) as the basis for identifying our achievements since FY2000, and formulating our outcomes for FY2006 – FY2008. Details regarding the components of the quadrants are provided in Section II, "The Past, Present, and Future – Where we are Going", which follows.

Process Used to Develop the FAA IT Strategy Fiscal Years 2006-2008

The Strategy and Investment Division (AIO-20) coordinates the development of an IT Strategy that addresses emergent technologies; aligns Departmental, agency Line of Business and Staff Office strategies; and establishes roles, responsibilities and governance within the framework of Enterprise Architecture. AIO-20 executed a structured process for this activity, which included the following:

- **Develop a framework for documenting the FAA IT Strategy**
  Develop an annotated outline and framework for the FAA IT Strategy with descriptions of the contents expected and the criteria for the document's approval and signature.

- **Meet with AIO Management Team, CIO Council, and Information Technology Executive Board**
  Facilitate meetings with the AIO Management Team, CIO Council, and the Information Technology Executive Board (ITEB) to discuss approach and solicit input on the corporate IT strategy.

- **Develop Draft FAA IT Strategy Fiscal Years 2006 – 2008**
  Develop and distribute an initial draft document, based on meetings listed in bullet above.

- **Individual Meetings**
  Discuss draft IT strategy with members of the IT community.

- **Develop Final FAA IT Strategy Fiscal Years 2006-2008**
  Vet the document with members of the IT community and update, as necessary.

- **Approval**
  Obtain signature approval from the Administrator and members of the Information Technology Executive Board. Obtain agreement from members of the CIO Council and their Assistant and Associate Administrators that their individual business plans will support the FAA IT Strategy.

Document Overview

The section that follows, *Section II – The Past*, *Present, and Future*, provides an overview of the history of IT strategy in the FAA, an inventory of accomplishments to date, and the approach that was used to define the IT strategy provided in this document. *Section III – The Challenge*, provides an inventory of the business drivers for change in FAA IT and how they influence the future direction. *Section IV – Vision, Outcomes, and Goals, su*mmarizes the corporate IT vision, outcomes, and goals for the future direction. How we achieve the vision, outcomes, and goals is provided in *Section V -- Corporate IT Initiatives for FY2006 – FY2008*. In *Section VI –- IT Initiatives for FAA Lines of Business (LOB)*, the LOBs have provided their own action plans for achieving the vision, outcomes, corporate IT goals, and initiatives described in Section V. *Section VII – Monitoring and Controlling the IT Strategy*, describes the management activities that will be performed to ensure that the FAA IT strategy achieves its objectives. There are three appendices. Appendix I contains an inventory of source documents used to perform this task. Appendix II provides the acronyms and abbreviation used in this document. In Appendix III, the FAA strategic goals are linked with FAA IT goals.

How the Document will be Used and Maintained

The FAA IT Strategy for Fiscal Years 2006-2008 will be incorporated into the life cycle for related agency documents (i.e., the FAA Flight Plan, LOB and SO Business Plans, LOB and SO Budgets and the Information Systems Security (ISS) Strategic Plan. *Figure 1: Document Links and Dependencies,* follows below and is a graphical depiction of how the FAA IT Strategy fits into the overall planning life cycle.

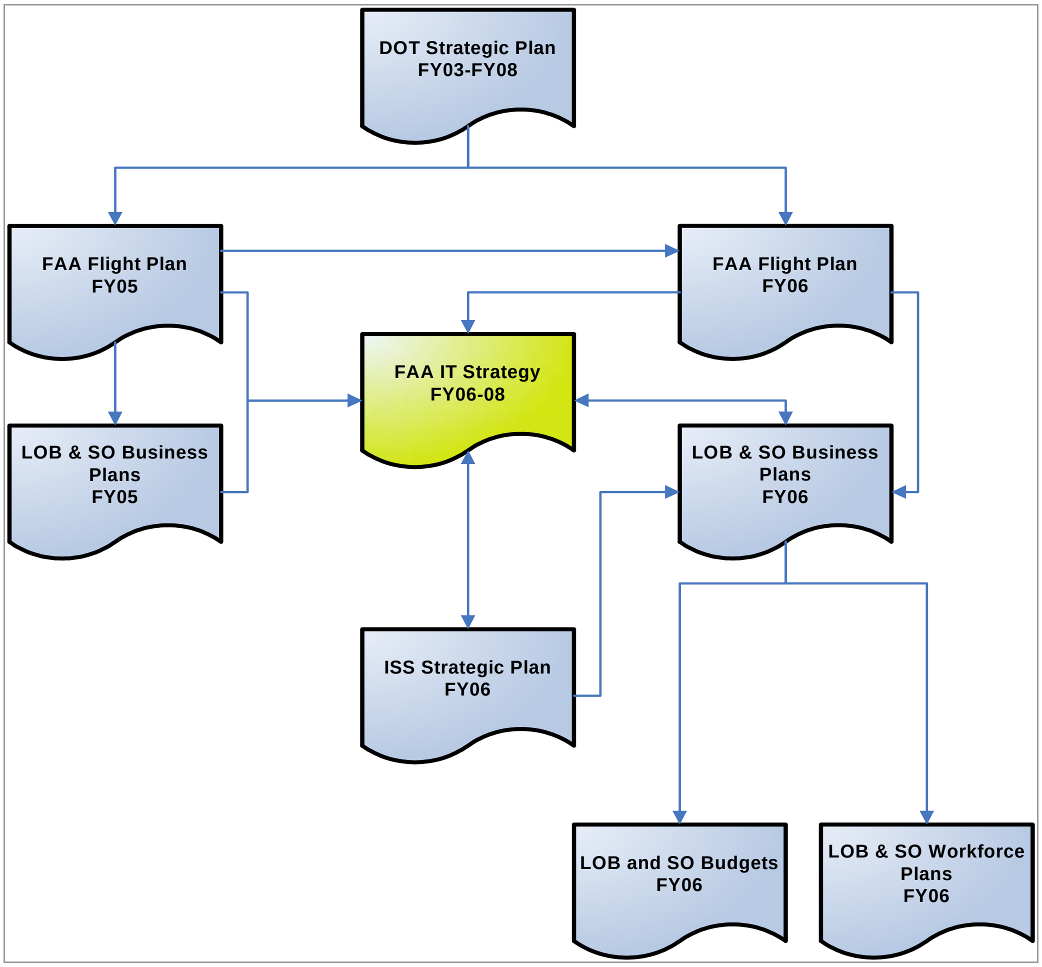

DOT Strategic Plan FY03-FY08
FAA Flight Plan FY05
FAA Flight Plan FY06
FAA IT Strategy FY06-08
LOB & SO Business Plans FY05
LOB & SO Business Plans FY06
ISS Strategic Plan FY06
LOB and SO Budgets FY06
LOB & SO Workforce Plans FY06

Figure 1: Document Links and Dependencies

The document is expected to undergo change throughout its three-year life. After delivering the previous document, FAA IT Strategy Fiscal Years 2003-2005, we learned that the strategy requires on-going modification. Because the business and technology landscapes change rapidly, the strategy must be revised to meet new challenges as they arise. Therefore, we will put ongoing execution, monitoring and control activities in place to ensure that the IT strategy for FY06-08 is managed, monitored and updated, as necessary. Section X – *Monitoring and Controlling the IT Strateg*y, describes the management activities that will be performed to ensure that the FAA IT strategy achieves its objectives.

II. The Past, Present, and Future

How We Got Here

This document will be the third FAA IT strategy. The first IT strategy covering 2000 – 2002 was developed shortly after the FAA CIO arrived and laid out the expectations of how the CIO's office, working with the rest of the agency, could add value to the FAA. That strategy emphasized policy, process, and investment and laid out an approach to IT security, data management, process engineering, and capital planning. The strategy set the groundwork for the future and established a budget line. The CIO used as an important symbol a "pyramid" – to illustrate the five- layered approach to information security, as depicted below in *Figure 2*:

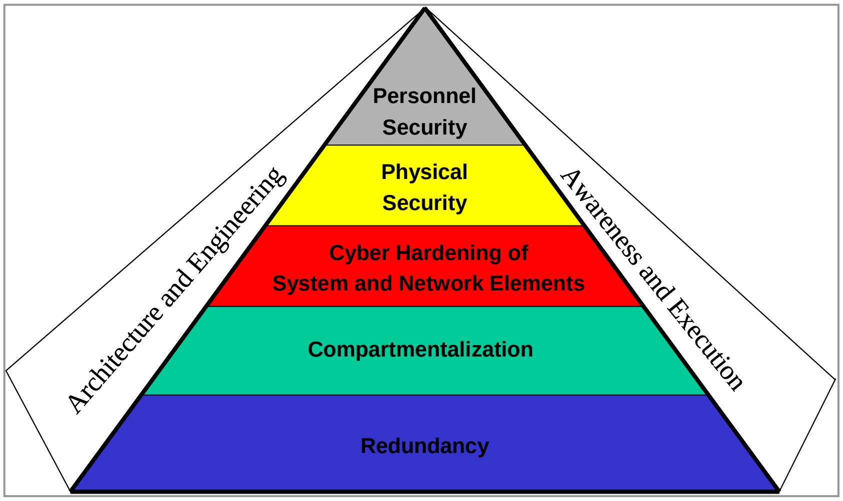


Figure 2: The Pyramid Approach to IT Security

The second strategy, developed in 2002 in conjunction with the newly formed CIO council, and covering FY 2003-05, focused on IT security, business value, and e-government. FAA was successful in all three areas – as evidenced by the grade of A- in FISMA and being seen as leaders in IT security; helping the DOT become the first Department to achieve "Green" in the E-government section of the President's Management agenda; and getting all exhibit 300s off the watch list in the President's budget this year. The icon was the "android", which represented a transition from just prevention to prevention and recovery. *Figure 3* follows and provides a graphical representation of this icon.

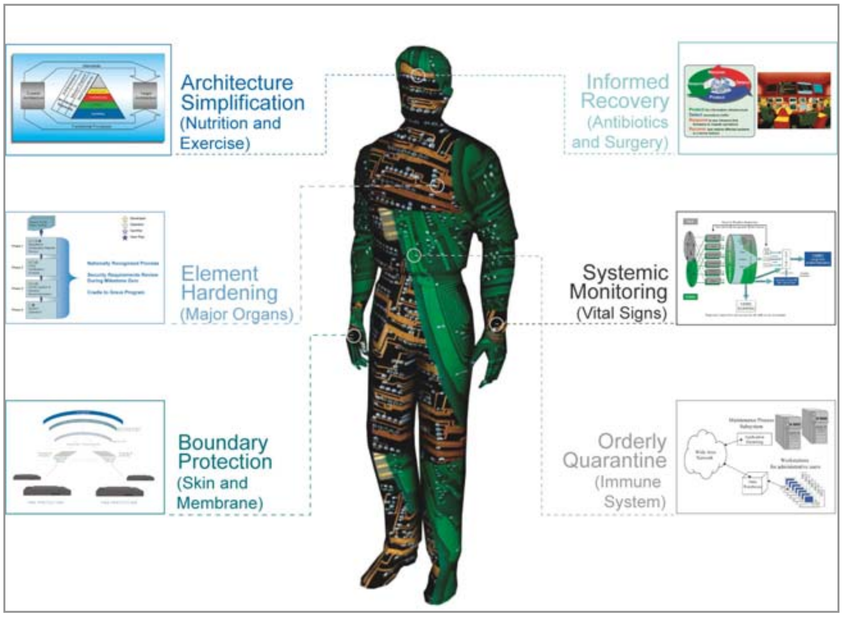


Figure 3: Cyber-Security Android Model

What We Have Accomplished

The timeline below provides an inventory of accomplishments achieved in FAA IT, since fiscal year 2000:

FY2000 – FY2002

- Established an effective Information Systems Security Program
- Established an agency Data Management Program and deployed a meta data repository
- Developed an ISS Architecture
- Created the FAA integrated Capability Maturity Model (FAA-iCMM) and began transitioning organizations from using iCMM Version 1 as their source of guidance for process improvement to using iCMM Version 2
- Established CIO Council, which includes representatives from each of the major business units and staff offices
- Improved the operations, security, accessibility, and content management of the FAA website in support of E-Government.

- Got to “green” in e-Government
- Initiated a series of corporate-wide procurements in data management and security, to reduce costs
- Awarded contract for FAA Telecommunications Infrastructure (FTI)
- Commenced Portfolio Management initiative
- Completed over 60 Security Certification and Accreditation Packages (SCAPs)
- **2003-2005 FAA Information Technology Strategy issued**

FY2003 -- FY2005

- Commenced development of a workable, streamlined information technology architecture
- Published version 4 of the ISS architecture
- Initiated IT Cost Control Initiatives (Web server consolidation, blanket purchase agreements (BPAs) and enterprise license agreements (ELAs), Desktop Standardization, etc.)
- Developed an Android Cyber Defense Model
- Enhanced WAN services via FTI
- Established NASE Web Portal
- Removed computer security from the IG’s material weakness list
- Established CONOPS for internet services
- Established Information Technology Executive Board
- Achieved passing scores on all 29 IT Exhibit 300 programs
- Modified AMS to base investment decisions on Exhibit 300 business cases
- Consolidated Web Hosting Facility
- Established operational standards for IT, led by the CIO Council
- Commenced IT Asset Baseline initiative

- Conducted annual meetings for IT specialists across the enterprise

- Published Safety and Security Extensions to the Integrated Capability Maturity Model

- Achieved A- score on the Federal Information Security Management Act (FISMA) Scorecard

- Became the first secretary-level agency in Government to achieve ‘green’ in e-Government

- Implemented corporate desktop standards for administrative and mission support domains that have provided opportunities for consolidation and resulted in cost savings.

- FAA voted one of the best places to work in Federal IT, based on the responses to the June 2005 Federal Computer Week survey on the climate within agencies for IT workers.

- **Issued 2006-2008 Information Technology Strategy**

Where We Are Going

The third FAA IT Strategy will be “outcome-driven”. The shift toward outcome-based FAA IT is analogous to the total quality movement in business and manufacturing. It reflects a belief that the best way for individuals and organizations to get where they're going is first to determine where they are and where they want to be--then plan backwards to determine the best way to get from here to there. To do this, we looked at FAA’s IT resources in the form of four quadrants, in order to formulate the end state for each in 2008. This approach is graphically depicted in *Figure 4: Moving into the Future*.

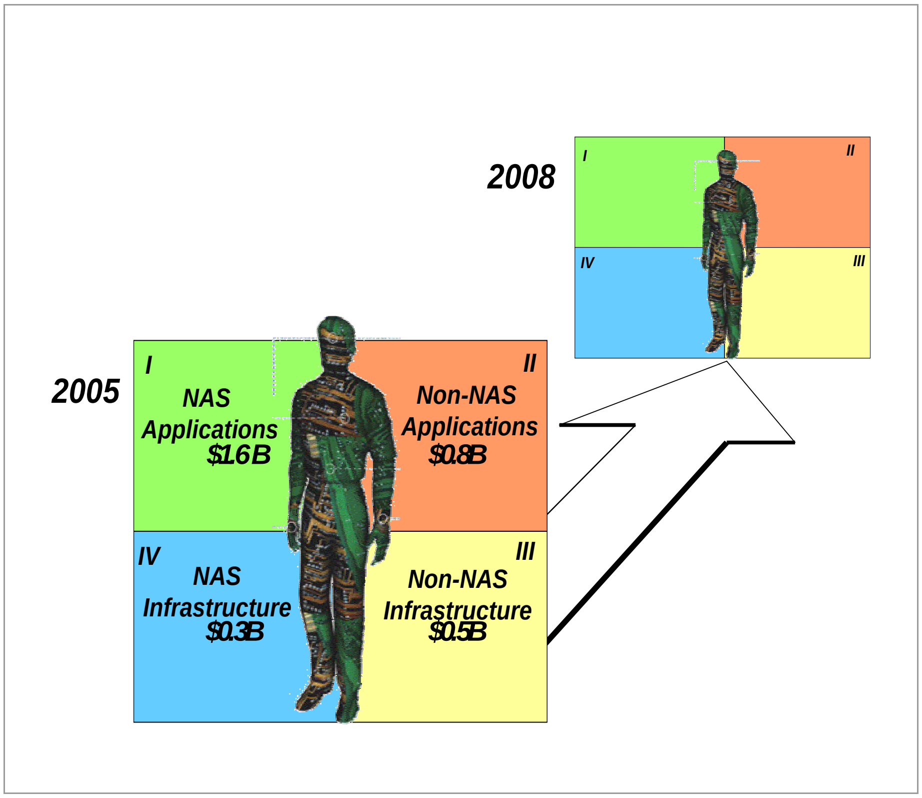


Figure 4: Moving into the Future

In this approach, we separate IT conveniently into NAS versus Non NAS, and applications versus infrastructure. The four quadrants are:

- **Quadrant I – NAS Applications (Programs)**
  This quadrant consists of all NAS applications (e.g., ASDE-X, ASR-9/11, ATOP, ECG, ERAM, ITWS, STARS, TAMR, URET, VSCS, WAAS, etc.), along with software development, testing, special equipment, and human capital (e.g., personnel, contractor costs, training/certification, etc.) that directly support the development and maintenance of NAS applications.

- **Quadrant II – Non-NAS Applications (Programs)**
  Quadrant II consists of all Non-NAS applications (e.g., CAS, DELPHI, SWIFT, NEXGEN, ASKME, SASO, etc.), along with software development, testing, special equipment, and human capital (e.g., personnel, contractor costs, training/certification, etc.) that directly support the development and maintenance of NAS applications.

- **Quadrant III – Non-NAS Infrastructure**
  Non-NAS Infrastructure contains desktops, desktop software, data centers, websites, servers, LANs/WANs and other telecommunications, help desk equipment, configuration management, information systems security, enterprise architecture,

capital planning and other components and processes that directly support the operation of Non-NAS applications, in addition to human capital. The FAA Telecommunications Infrastructure (FTI) is an integrated suite of products, services and business practices that spans the NAS and Non-NAS infrastructures.

- **Quadrant IV – NAS Infrastructure**
  NAS Infrastructure contains desktops, desktop software, data centers, websites, servers, LANs/WANs and other telecommunications, help desk equipment, configuration management, information systems security, enterprise architecture, capital planning and other components and processes that directly support the operation of NAS applications, in addition to human capital. The FAA Telecommunications Infrastructure (FTI) is an integrated suite of products, services and business practices that spans the NAS and Non-NAS infrastructures.

We made an initial estimate of what we spend annually in each category, which is substantial, and probably an underestimate. Our challenges are different for each quadrant, and we will discuss these in the section that follows, *Section III: The Challenge.*

III. The Challenge

Business Drivers for Change

Several factors are driving the need for changes to FAA IT. *Figure 5: Key Business Drivers for Change in FAA IT*, follow below and is a graphical depiction of these competing factors.

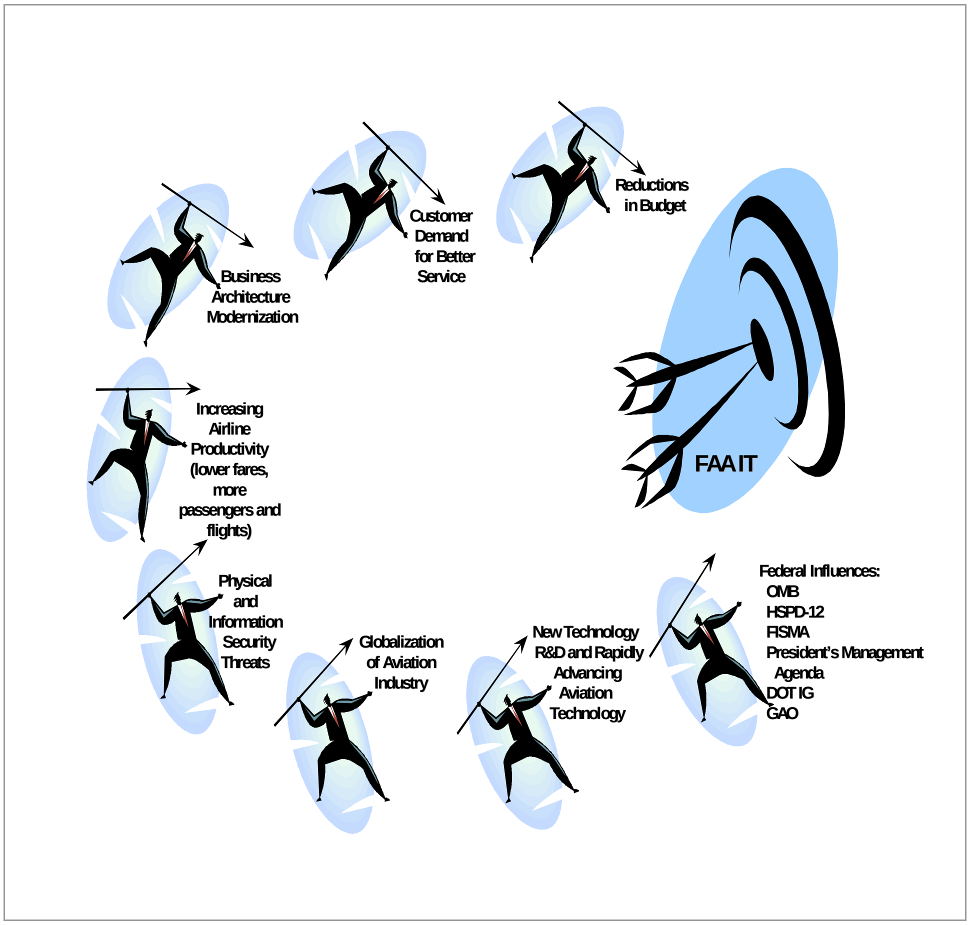

Reductions in Budget
Customer Demand for Better Service
Business Architecture Modernization
FAA IT
Increasing Airline Productivity (lower fares, more passengers and flights)
Physical and Information Security Threats
Globalization of Aviation Industry
New Technology R&D and Rapidly Advancing Aviation Technology
Federal Influences:
OMB
HSPD-12
FISMA
President's Management Agenda
DOT IG
GAO

Figure 5: Key Business Drivers for Change in FAA IT

The complete set of business drivers are classified as follows:

- Internal Influences – are summarized as reductions in budget and gains in productivity, aging workforce, needs for a mobile workforce, corporate restructuring and rightsizing, business architecture modernization initiatives and customer demand for better service.
- Federal Influences – come from the White House, Office of Management and Budget (OMB), National Institute of Standards & Technology (NIST), Government Accountability Office (GAO), DOT Inspector General, E-Government, Federal Information Security Management Act (FISMA), and other Federal Government entities.
- External Influences – include continuing and more sophisticated physical and information security threats; new technology research and development and rapidly advancing aviation technology; increasing airline productivity and complexity, declining fares and increasing numbers of passengers and flights; globalization of the aviation industry; and industry trends, such as commoditizing IT, consolidation, real-time processing and web services; and other influences outside the FAA.

Internal Influences

A high priority for FAA is bringing agency costs under control. In the AIO Fiscal Year 2005 Business Plan, a key activity target is to "control IT spending so there is no real growth in the non-NAS IT budget and savings are identified for potential reinvestment (while maintaining the same, or improving, the level of service)". Over the next three years, as we achieve higher levels of performance in IT, as a result of consolidation and sharing of resources, we expect reductions in costs to be significant. Similar IT cost control targets appeared in other Line of Business and staff office business plans. This target currently influences *Quadrant III – Non-NAS Infrastructure*. Over the next three years, the same type of outcome will be achieved in all quadrants.

There are changes in the way our employees carry out their work, compared to three years ago. The workforce is more mobile and telecommuting has become an effective way for individuals in particular roles to achieve the stated objectives of their jobs.

Finally, there are several initiatives that involve the integration of related business processes and systems. Some examples are integration of personnel and payroll systems, integrated financial processes and systems, improvements in logistical and asset management systems, and others.

Federal Influences

In terms of federal influences, the President's Management Agenda affects what we need to achieve in *Quadrant II – Non-NAS Applications*, in terms of maintaining our performance on the electronic (e)-government initiative. At the same time, *Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Employees and Contactors*, may potentially affect all quadrants, which results from implementing a compliant solution for providing employees and contractors with logical access to FAA's computer systems. As a result of GAO-04-822 and GAO-05-207 (GAO High Risk List), FAA is required to put more oversight of operational systems in place, which has the greatest influence over *Quadrant I -- NAS applications* and *Quadrant IV – NAS Infrastructures*.

External Influences

Continuing and more sophisticated information security threats, in the form of asymmetric warfare, have the potential to affect all quadrants, in terms of securing our applications and infrastructures. It is imperative that we implement the "right side of the Android model", in terms of recovery, real-time monitoring, and quarantine.

Aviation demand has been significantly affected by a number of events over the past several years. As a result, total activity across the NAS, i.e., landings, arrivals, and en route handover counts, are still about 4 percent below 2000 levels, while passenger activity is 15 percent lower than the 2000 peak. However, these aggregate totals do not reflect other developments of interest in the aviation industry. The global trend of airline deregulation and privatization, combined with technological improvements, has increased airline productivity. Combining this with the success of "low-fare" airlines, average fares decrease and the number of passengers per year worldwide increases. To meet this increase in demand, the FAA, the airport authorities, local governments, researchers, suppliers, the DOD, and other members of the aviation community, must continue their efforts to jointly improve the capacity and the performance of the air transportation system through change to the NAS Architecture, which includes the applications and infrastructure in *Quadrant I – NAS Applications* and *Quadrant IV – NAS Infrastructure*.

Description of the Challenge

> *"The challenge for FY2006 through FY2008 is to build up the capabilities needed to maintain our gains in cyber security, business value, and e-government, while achieving leadership in the areas of IT performance, cyber security, and the management of IT programs in the future"*

The challenge can best be met by determining a realistic, sound and cost-effective vision that enables the FAA IT community to bring about ambitious changes for the next three fiscal years and beyond. This vision is documented in Section IV, which follows.

IV. Vision, Outcomes, and Goals

More than ever, technology must be considered an *enabler* of business strategy, and not the strategy itself. Organizations today must plan appropriately to maximize the potential that technology can offer their organization.

Corporate IT Vision

"Creating an environment that makes information technology a business enabler for the FAA – providing secure and efficient capability to store and exchange the agency's critical information!"

Outcomes

We are aiming at two sets of outcomes:

(1) **Hold the gains we have achieved in cyber security, business value, and e-government.**

(2) **Achieve a leadership position in critical areas of IT including business value, IT performance and cyber security while controlling costs, standardizing and consolidating where appropriate, and building the capabilities to operate effectively and securely in the future.**

Corporate IT Goals

The FAA IT community is ready to meet the challenge of moving to the next generation capability of corporate IT, defined in the corporate vision. We have established three goals that complement the strategic goals set forth by the Flight Plan, the Lines of Business and the Staff Offices and focus on the need to meet the opportunities that today's technology can provide for our customers.

The three goals are:

1. ***Business Value and Performance***
   "Business Value" means that FAA IT is aligned with the business, its

performance is measured, its resources properly allocated and its risks mitigated. IT optimization and performance initiatives are included in this goal, and are focused on generating significant savings in information technology costs, while maintaining and/or improving the delivery of IT services to users. Also contained in this goal is the Flight Plan goal of getting the NAS Modernization Programs off the GAO High Risk list by 2008 and the business plan goal of ensuring that our Exhibit 300 business cases receive passing scores from OMB.

2. ***Cyber Security***
   The cyber security goal for FY2006 – FY2008 includes the following characteristics: maintain the FISMA grade, achieve zero cyber security events that significantly disable or degrade FAA service, and complete the Android model. Specific details for this goal are provided in the FAA Information Systems Security Plan FY2006 – FY2008 (Draft, August 2005), which is referenced in Appendix I, item 38.

3. ***E-Government***
   The goal for "E-Government" requires us to maintain "green" on E-government initiatives in the President's Management Agenda scorecard and provide support, as appropriate, in the other three areas.

Appendix IV: Links between FAA Strategic Goals and Corporate IT Goals depicts how the corporate IT goals directly and indirectly support the FAA goals in the Flight Plan. The rest of this section provides the high level objectives for moving into the future from FY 2006 through FY 2008.

Achieving the Corporate IT Goals

In order to design the roadmap for the next three fiscal years, we looked at the corporate IT vision for FY2006 – FY2008, the goals we want to achieve, and the federal mandates, external influences and internal influences that are driving the need for change. These factors were analyzed, in terms of the quadrants that were previously introduced and are depicted below in *Figure 6: Quadrants*.

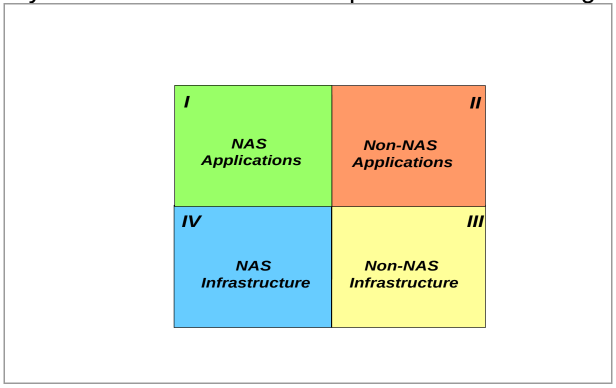
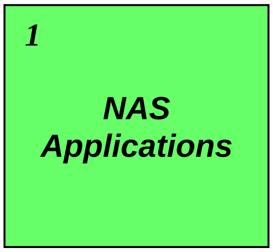


Figure 6: Quadrants

Quadrant I – NAS Applications/Programs



In this quadrant, FAA IT focuses on business value and IT security. To achieve business value, exhibits 300s for the top 25 major IT investments have continued to receive passing grades, to date. In the future, exhibit 300s for all major IT investments will receive passing grades. In addition, earned value management (EVM), a project management technique for estimating how a program/project is doing in terms of its budget and schedule, will be implemented agency-wide by FY2007. There will be systematic monitoring of variances and performance for compliance. Finally, an IT portfolio management program will be put in place to ensure that senior managers can evaluate a collection of programs/projects to see how they are performing, measure how well the programs/projects fit the agency's strategic plan and determine return on investment and risk level. All of these activities are in support of the Flight Plan goal of making sure that the FAA National Airspace Modernization Program is removed from GAO’s High Risk List by 2008

The following activities are currently performed to achieve the IT security goal: utilizing a comprehensive process for producing system security certification and authorization packages (SCAPs) to ensure that all disciplines touching an FAA system—computer, communications, emissions, operations, information, physical, personnel, industrial, and administrative—are evaluated, protected, and documented; systematically executing vulnerability assessments to identify and evaluate vulnerable FAA IT resources that, if exploited, compromised, damaged, or destroyed, could critically impair the agency’s ability to operate; and, supporting the goal for zero cyber security events that disable or significantly degrade FAA service. Along with these activities the IT security goal for FY2008 also includes development of both sides of the Android model (i.e., prevention and recovery from attack).

Quadrant II – Non-NAS Applications

11

Non-NAS Applications

In Quadrant II, the current focus is on business value, IT security, and E-government. To achieve business value, exhibits 300s for all major IT investments have continued to receive passing grades, to date. In the future, exhibit 300s for all major IT investments will receive passing grades. In addition, earned value management (EVM) will be implemented agency-wide by FY2007. Finally, there will be systematic monitoring of variances and performance for compliance.

Like Quadrant I, the goal for IT security has been achieved by utilizing SCAPs, performing vulnerability assessments, and supporting the cyber security goal for zero cyber security events that disable or significantly degrade FAA service. These activities will continue. However, a critical priority for IT security in the future is to achieve cyber situational awareness, which is the accurate perception of the operational and environmental factors that affect the network's security state and being armed to take actions that balance security and network availability. For FY2006 – FY2008, developing both sides of the Android model and achieving cyber situational awareness will be achieved.

The E-government goal in the President's Management Agenda applies to Quadrant II. The FAA has helped the DOT become the first Department to achieve "Green" in the E-government section and will continue to do so. In addition, we have supported electronic DOT-wide systems and achieved some system sun setting. In the future, we will identify additional systems for sun setting, as well as complying with government-wide initiatives.

During the FY2006 – 2008 timeframe, we will achieve IT cost controls goals for the Non-NAS applications by developing and maintaining an accurate IT inventory.

Quadrant III – Non-NAS Infrastructure

111

Non-NAS Infrastructure

Current goals in Quadrant III are IT security and some IT cost control. The IT security goal is achieved by systematic execution of vulnerability assessments and supporting the cyber security goal for zero cyber security events that disable or significantly degrade FAA service. To achieve the IT security goal for FY2006 – FY2008, developing both sides of the Android and achieving cyber situational awareness will supplement these activities. And, simplification to support security will be designed and put in place.

Activities to achieve IT cost control goals in the Non-NAS infrastructure began in December 2004, as a result of the off-sites meetings held by AIO and the CIO Council. The CIO Council agreed to implement six projects, called the *CIO-6* (i.e., server consolidation, help desk consolidation, LAN standards, Web consolidation, Architecture, and consolidated active directory) designed to consolidate and streamline key components of the infrastructure. These projects will continue in the FY2006 – 2008 timeframe. Additional activities will be carried out to meet the FAA goal for cost control, which include: total asset visibility that could result in cost reductions of 10% or higher; infrastructure streamlining; enterprise licenses; implementation of shared services; and, total information awareness.

Quadrant IV – NAS Infrastructure

1V

NAS Infrastructure

In Quadrant IV, the current focus is on IT security, which includes the systematic execution of vulnerability assessments and supporting the goal of zero cyber security events that disable or significantly degrade FAA service. Like Quadrant III, the IT security goal for FY2006 - FY2008 is to continue the ongoing activities as well as development of both sides of the Android model and achieving cyber situational awareness.

In addition, during the period from FY2006 – FY2008, activities will be carried out to meet the FAA goal for cost control, which includes: total asset visibility that results in cost reductions of 5% or higher;

infrastructure streamlining; enterprise licenses; and, investigating the potential for shared services.

Section V – Corporate IT Initiatives for FY2006 – FY2008 specifies how we will achieve the vision, outcomes and corporate IT goals discussed herein.

V. Corporate IT Initiatives for FY2006 – FY2008

Achieving the corporate IT vision will require structural, policy, and process changes!

Outcomes: First Set

“Hold the gains we have achieved in cyber security, business value, and e-government.”

We will achieve this set of outcomes by introducing new tools, methods, and processes that enable us to move beyond current accomplishments, in order to make information technology a business enabler for the FAA. The strategies and associated initiatives that we will perform to accomplish the first set of outcomes are listed below. Each strategy is linked to one of the three corporate goals (i.e., Business Value and Performance, Cyber Security, and E-Government).

Business Value and Performance: Evolve and Mature the Exhibit 300 Development and Review Process

To successfully execute this strategy, we will keep our commitments to OMB to move towards full implementation of earned value management (EVM) within the agency by the end of FY 2007. In addition, we will move the agency towards level 3 implementation of the IT Investment Maturity model as we agreed to do in our response to GAO. We will work with the virtual Value Management Office within AIO-20 to develop processes to manage the entire IT portfolio. This requires complete visibility of the application portfolio in each line of business or staff office and identifying all programs/applications and IT investments. In compliance with GAO, the development of these strategic linkages will depend upon a stronger architecture program for guiding system modernization efforts.

Business Value and Performance: Link OMB 300 Development and Review, Enterprise Architecture, and Program Execution

To move into the future in providing business value, we will implement a well- managed and controlled process whose interdependencies create a check and balance mechanism for investments and enterprise-focused technology decisions. In this process, enterprise architects will collaborate with systems engineers to create new capabilities for program execution and will work with OMB 300 staff to ensure that investments support the direction of the FAA Enterprise Architecture. Program execution will be linked to and supported by business process improvements. The FAA has been achieving more effective and efficient processes and process improvement by using the FAA integrated Capability Maturity Model® to guide its improvement efforts. In the future FAA will continue to use FAA-iCMM®, as well as equivalent enterprise improvement methodologies and standards (e.g., ISO 9001:2000, Six Sigma, etc.) *Figure 7: Strategic Linkages,* follows and depicts the concept for this new process.

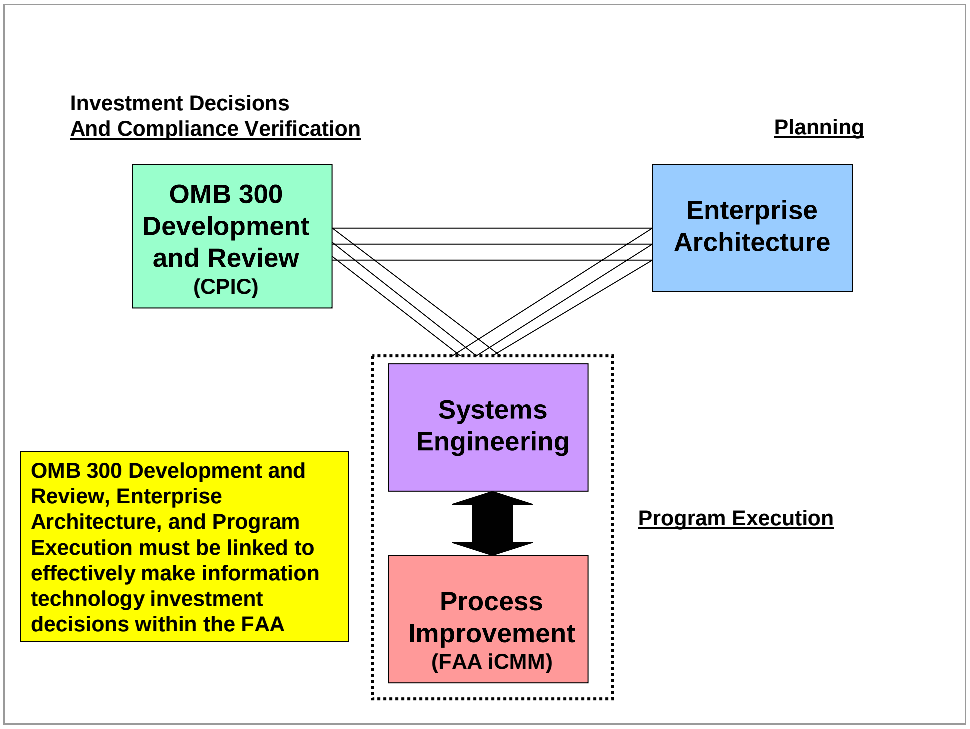

Investment Decisions
And Compliance Verification
Planning
OMB 300 Development and Review (CPIC)
Enterprise Architecture
Systems Engineering
Process Improvement (FAA iCMM)
Program Execution
OMB 300 Development and Review, Enterprise Architecture, and Program Execution must be linked to effectively make information technology investment decisions within the FAA

Figure 7: Strategic Linkages

Analysts creating and reviewing the 300's need a blue print (i.e., Enterprise Architecture) to use to evaluate the 300's and ensure that the programs support the overall enterprise. In addition, the Analysts who create and review the 300's need to collaborate with systems engineers to obtain the content for the 300's. Systems engineers need to collaborate with the architects who provide the capabilities that need to be created to support the enterprise. And, the architects depend on the capital planning and investment control process (CPIC), from which the 300's are produced. Within the LOBs and SOs, this process can be used for IT investments that do not require an exhibit 300.

Specific initiatives that will be performed over the FY2006 – FY2008 timeframe include the following:

FY06

- **Establish an Architectural Review Board within the FAA acquisition process**
  The architectural review board will participate in the acquisition process reviewing program compliance to the FAA's enterprise architecture. ARD is expected to be in the FAA Acquisition Management System (AMS) by January 1, 2006.

FY07 - FY08

- **Monitor program compliance with the enterprise architecture and provide feedback into the CPIC and acquisition processes**

- **Enhance the existing FAA configuration management process**

Note: Additional information on this initiative FY2006 is provided in the FAA ARD-1 500 Day Plan (dated August 10, 2005), which is referenced in Appendix I, item 35.

Cyber Security: Evolve and Mature Essential Elements of the FAA ISS Program in Order to Maintain an "A" Grade in FISMA

This strategy supports the first set of outcomes in the IT strategy by taking careful steps to hold cyber security gains in spite of a moving environment. This requires leadership and initiatives that actively learn from, and build upon, accomplishments. As such, major ISS program elements will continue to be supported. However, holding the gains is a moving target, based on ever-evolving threats, the continuing modernization of FAA information systems and information technology infrastructures, more comprehensive mandates, and increasing Federal Government oversight. Strategic initiatives that "hold the gains" must go beyond "maintenance" to ensure the FAA acquires the resilience needed to meet changing threats and mandates. In FY06, initiatives will continue to achieve challenging certification and remediation related targets that were started in previous years, and will adapt ISS policy and standards to reflect new FISMA and OMB requirements. Moreover, the FAA will put in place a multi-dimensional compliance program to ensure we are holding the gains". In FY07 and FY08, the program will continue to build on this groundwork, evolving current program elements and deepening the agency's preparedness to resist an attack, manage vulnerabilities, and maintain secure boundary defenses. Initiative opportunities include both agency-wide and local efforts to improve security throughout system development life cycles. Efforts are planned to develop agency-wide policies, templates, handbook products, and mechanisms for incident response and reporting, information security knowledge management, and common vehicles for acquiring important ISS acquisition vehicles, such as "Malware". The specific initiatives for carrying out this strategy are provided below:

FY06

- **Ensure that All Operational Systems Complete C&A or Self-Assessment**
  Ensure that all operational systems in the information systems inventory complete current certification and accreditation (C&A) or undergo a self-assessment if full C&A is not required.

- **Remediate High Vulnerabilities (DISP)**
  Remediate targeted high vulnerabilities identified in the DOT Portal (DISP) as of October 1, 2005 with a completion date of September 30, 2006.

- **Ensure One-Third of System Inventory**

Completes Recertification
During the course of FY2006, ensure that one-third of the information systems inventory undergoes recertification with completion by September 30, 2006.

- **Achieve a “4” or Better on the Security Portion of All Exhibit 300s**

- **Develop, Document, and Exercise an ISS Compliance Program**
  Develop, document, and exercise the FAA ISS Compliance Program. The program will contain management plans, clear roles and responsibilities, and mechanisms to ensure compliance with policies, procedures, and standards, including monitoring the adequacy of selected security controls, as defined in FIPS 200. Complete a plan for exercising the FAA ISS Compliance Program for FY2006 – FY2008.

- **Provide ISS Awareness and Specialized Training**
  Provide refresher and specialized ISS training for 100 percent of FAA key personnel as identified by LOBs/SOs. Provide awareness training to all FAA employees and contractors who support the IT operations and assets of the agency. The training will be tracked and reported to the *FAA Information Security Business Portal*.

- **Develop Baseline Information Security Requirements**
  Cooperate with DOT to establish baseline ISS security requirements by September 30, 2006.

- **Develop a NIST Compliant C&A Process**
  Develop and document a C&A process that complies with NIST guidelines within six months after FAA ISS Program Order 1370.82a is published.

- **Achieve 0.10 or Fewer High Vulnerabilities (SANS top 20)**
  By September 30, 2006, achieve 0.10 or fewer high vulnerabilities, as measured against the SANS (SysAdmin, Audit, Network, Security) Institute top 20, for targeted network servers.

- **Establish Memorandum of Cooperation on Cyber Security in Concert with FAA’s AIA International Plans**

Establish memorandum of cooperation on cyber security with foreign air traffic management organization in concert with FAA's AIA international plans.

FY07 – FY08

- **Continue FY06 Initiatives**

- **Ensure Mandated ISS Program Assessment and Control Capabilities**
  Continue to build and mature the FAA ISS Program through the development of ISS policy and standards as required by FISMA, NIST and other mandates, through the execution of life cycle control recommendations identified by the FY06 ISS Compliance program, and through improved ISS planning, budgeting, information sharing, and training efforts.

E-Government: Maintain "Green" on E-government Initiatives in the President's Management Agenda Scorecard

To stay "green" we will need to provide capability to transact business electronically with citizens (G2C), business (G2B) or other parts of government (G2G), and consider sun setting redundant systems. The main objective for this goal is to provide the capability for external customers and employees to transact business with the FAA electronically. This will be accomplished through continued improvement of service delivery processes and capabilities, and development of project portfolios aimed at key customer groups of citizens, businesses, other government agencies, employees, and internal efficiency and effectiveness. E-government is one of the five main goals of the President's Management Agenda and mandates the use of "Best IT Management Practices." These are embedded into every goal and objective within the FAA IT strategy.

The FAA Office of Communications (AOC) will take a leadership role in providing web services that reach out to, and connect with, both internal and external customers. These services will be focused on customers needs and provide transactions that process quickly and efficiently. Aviation Safety will be taking the lead to build systems for external customers/business partners that promotes and enables the sharing of data, no matter who owns it. These efforts will be preceded by business process reengineering and improvements that result in more efficient performance and increased agility to meet new demands from industry.

We are already working with the Department of Transportation on accomplishing significant Presidential Initiatives such as Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors[1]; E-Travel[2]; and, Enhanced Human Resource Initiative (EHRI)[3]. FAA Human Resources Management (AHR) is working aggressively to implement a compliant Electronic Official Personnel Folder (EOPF), which is a component of EHRI. EOPF will be designed to assemble and maintain a collection of electronic documents and forms covering the complete Federal civilian employee's personnel history and current status. AHR plans to make their solution available to other Federal entities, on a cross-agency basis.

On August 2, 2005, OMB mandated that all U.S. Government agencies transition their Internet backbones to Internet Protocol Version 6 (IPv6) by June 2008[4]. By this deadline, all agency infrastructures (network backbones) must be using IPv6 and all agency networks must interface with this infrastructure. Conversion to IPv6 is expected to create a significant impact on the FAA Telecommunications Infrastructure (FTI) and all LOB Chief Information Officers. In addition, this mandate is unfunded. In FY06, FAA will coordinate with the Department of Transportation to stand up a joint program office, establish contracts, and complete the required inventories and migration risk analysis.

Over the next 18 to 36 months, we will improve internal efficiency and effectiveness by eliminating redundant business functions and consolidating to those determined by OMB to be Centers of Excellence for conducting government business functions. For example, on October 16, 2005, the FAA will migrate to the Federal Personnel Payroll System (FPPS). The goal of the FPPS Migration is to streamline and consolidate payroll services across the Federal Government.

[1] http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[2] http://www.whitehouse.gov/omb/egov/2003egov_strat.pdf

[3] http://www.whitehouse.gov/omb/egov/c-4-3-ehri.html

[4] http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

Outcomes: Second Set

"Achieve a leadership position in critical areas of IT including business value, IT performance and cyber security while controlling costs, standardizing and consolidating where appropriate, and building the capabilities to operate effectively and securely in the future."

We will achieve this leadership position by identifying and implementing the right programs that ensure we achieve a unified and more effective approach for managing information technology across the agency. The strategies and associated initiatives that we will perform to accomplish the second set of outcomes are listed below. Each strategy is linked to one of the three corporate goals (i.e., Business Value and Performance, Cyber Security, and E-Government).

Business Value and Performance: Information Technology Optimization and Performance

IT Optimization and performance is an ***enterprise-wide*** approach to becoming "best in class" in IT while supporting the "Organizational Excellence" cost control goal in the FY05-FY09 Flight Plan and the second set of outcomes in the corporate IT vision. The real objective is for the agency to achieve high performance in IT by providing the best services at the best cost. This initiative began in FY2005 and will continue as an ongoing operation over the three-year life cycle for this IT strategy. By promoting the cooperative use of IT assets and services across FAA and making wise investments that improve IT assets and services, the initiative is expected to yield savings in operational costs over time, as well as providing many additional benefits, as follows:

- Improved support of agency programs
- Better security and reduced infrastructure risk
- More effective use and management of IT assets and investments
- Diminished duplication of IT services
- Augmented delivery of government services to benefit the public (E-government)

IT Optimization and Performance contains the following activities:

(1) ***Develop Agreed-Upon Metrics for a High Performance IT Enterprise (FY2005 – FY2006)***

Research into best practices in efficient and effective management of IT in the federal and local government and private sector organizations will be performed, in order to identify a set of outcomes and metrics that characterize high performance IT. For example, several years ago, key performance measures for IT in the Mobil Corporation included percentages related to: global system reliability, global system security, service and customer satisfaction, and cost accountability and people. In the *State of Michigan*, the IT community is measuring their performance against the following set of metrics and outcomes:

- 99.9% uptime for State of Michigan wide area network every year.
- Full suite of online services accessible to 80% of Michigan residents, even those who do not own computers.
- Comprehensive statewide technology disaster recovery plans for all critical systems.
- 90% of all intrusions and viruses are repairable within 2 hours.
- 100% statewide enterprise systems certified and accredited for proper security controls.

Based on the results of this research, the FAA IT community will work together to endorse a common set of metrics for high performance IT and will participate in routine reporting against these metrics for tracking performance.

(2) *Semi-Annual Review of IT Inventory (FY2006 – FY2008)*

This activity will be done in parallel with the metrics activity described above, and involves the ***development and ongoing management*** of the FAA IT inventory, which consists of:

- Programs
- IT services (e.g., Internet, Intranet, Desktop, Email, etc.)
- IT assets for each service
- Baseline costs
- Human capital

We will start with “architecture” as the basis for the IT inventory. AIO will work closely with each LOB/SO to make sure the IT inventory is current. Visibility into all agency IT programs, assets, and costs is required, and will give management the authority and the flexibility to promote efficiencies and make more informed budgetary decisions. We expect that the costs involved in developing and maintaining the IT inventory will ***significantly decrease over time***, as more automated tools are acquired and used.

Beginning in March 2006, AIO will conduct a review of the FAA IT inventory on a semi-annual basis, using automated simulation and optimization to guide decision-making. The results of these reviews will be provided to the ITEB, as the basis for changes that lead to greater efficiencies and performance, in line with the agreed upon metrics from activity (1) above. For example, the ITEB may make decisions on recommendations for the implementation of specific IT utilities or shared services, which are accompanied by best practices in service level agreements and delivery of services to users. Such services would not just achieve cost reduction, but would need to add value by improving management control and enhancing business performance.

(3) *Implement Optimized IT Inventory (FY2006 – FY2008 and beyond)*

An initial emphasis on infrastructure could provide a foundation for optimizing the FAA IT inventory, and focuses on the following areas:

- *Technical Infrastructure Consolidation/Improvement*

  Common infrastructure services could be consolidated across the enterprise and provided as "IT utilities" at technical domain levels, such as security, directory services, email, etc. Technical infrastructure decisions are already underway, in terms of servers, active directories, and help desks. For example, under the direction of the CIO Council, the ***FAA Directory Services Program*** will bring as many FAA computer systems as feasible under a single directory services structure and coordinate the migration of FAA network management to a more centralized model. A common directory services IT utility supports the FAA Flight Plan's Organizational Excellence goal, Objective 3 – "Make decisions based on reliable data to improve our overall performance and customer satisfaction. In addition, this program supports Homeland Security Presidential Directive #12 (HSPD-12) by facilitating common logical access to federally controlled information resources.

  Another important technical infrastructure improvement is to identify and implement Single/Reduced Sign-on projects for targeted systems, such as those already successfully implemented by FAA Airports (ARP). Single Sign-on (SSO) is a method that provides users with the ability to log in one time, getting authenticated access to all their applications and resources. This effort will streamline logical access process and procedures for targeted systems and significantly reduce the operational and budgetary cost of maintaining multiple passwords. The identification and justification of specific projects and the development of implementation plans for this effort are targeted for FY06.

- *Inter-LOB/SO Business Domain Consolidation*
  In order to promote the highest level of inter-LOB/SO sharing and leveraging of services, common business functions (e.g., budget, finance, etc.) will continue to be reengineered and provided as shared services for the business domains of NAS, Mission Support, and Administration.

- *Organizational Consolidation*
  LOBs/SOs could consolidate IT functions, as necessary, so that duplication is minimized. For example, in FY2005, FAA's Air Traffic Organization (ATO) transferred the operation of a co-located regional help desk to FAA Region and Center Operations (ARC). And, in the 4th quarter of FY2005, ATO requested that FAA Information Services (AIO) assist them to achieve a higher level of IT optimization. The results of this partnership will be shared across the enterprise.

(4) *Standards and Compliance (FY2005 – FY2008 and beyond)*

IT standards currently exist and more will be required to achieve the expectations for IT optimization and performance. Standards and compliance will focus on improvements in the performance of the IT infrastructure, rather than cost control. For example, the Data Management Policy establishes FAA data as an enterprise resource that must be managed from an enterprise perspective. The FAA Management Program focuses on building the framework to manage FAA data resources effectively and reliably. Data management is a key enabling activity for cost cutting initiatives in application consolidation, information quality, internal and external information sharing, and meeting the challenges of evolving Presidential and legislative mandates. Over the coming years, the Data Management Program will be building on its early successes in NAS data standardization. It will be expanding to meet the enterprise-wide data resource management needs and include all lines of business and staff offices. Actions taken to move the program forward include getting support from the CIO Council, establishing a cross-organizational process team to revise the process, establish an agency-wide data governance board, and revise the current data management order. The new governance board will be responsible for FAA-wide data management practices, co-chaired by AIO, AVS, ATO, and membership representing the entire agency. The revised order established the board and addresses the need for expanded information stewardship. Current details and direction for the program were presented to the CIO Council August 4, 2005 and the Information Technology Executive Board on September 8, 2005. CIO Council and ITEB briefing material, draft Data Management Order, and Draft Governance Board Charter are referenced in Appendix I, items 11, 34, 41, 42, and 42.

(5) ***Workforce Management, Training, and Development (FY2005 – FY2008)***

FAA will ensure that our IT workforce has the competencies, skills, and certifications required for the successful implementation of the agency's IT Strategy. Accordingly, the Office of the CIO and the Office of Human Resources Management partnered in conducting an IT workforce assessment. The end product was the development of an FAA IT Skill Gap Closure Plan that focuses on four specialized job activities: IT Project Management, IT Security/Information Assurance, IT Architecture (Enterprise), and IT Architecture (Solutions). Across government, IT workforce capabilities will be monitored as part of the President's Management Agenda, Human Capital Scorecard requirement to significantly reduce gaps in mission critical occupations and competencies. The Department of Transportation "Proud-to-Be III" goals require the FAA and other DOT operating administrations to report quarterly on progress in closing IT workforce skill gaps beginning fourth quarter FY2005 and continuing through FY2006 and FY2007.

Cyber Security: Develop Total FAA Cyber Situational Awareness in order to Enable the Right Hand Side of the Android Model

This strategy supports the second set of outcomes by building cost effective partnerships that advance critical areas of FAA IT, since information security is critical to business value, cost control, standardization, consolidation, and the development of future, highly secure, modernized FAA operations. From a cyber security standpoint, the FAA ISS program must keep pace with the security implications of a modernized, yet still complex, air traffic system by improving its layered protection scheme. We will accomplish this by building the "situational awareness" necessary to monitor critical and widespread system elements to more quickly detect and react to failures. The ultimate realization of this kind of capability is envisioned in the right side of the Android model.

For FY2006, strategic initiatives will expand security services for FAA ports of information egress and ingress, expand and accelerate flows of security data between internal and external organizations, and provide greater situational awareness for the role of the Computer Security Incident Response Center (CSIRC) in incident detection and response. For FY2007 – FY2008, planned initiatives will continue to move toward full situational awareness locally and across the enterprise. These initiatives will advance the understanding and use of appropriate situational awareness approaches and tools through careful investments and partnering arrangements to discover cost effective systemic monitoring techniques, such as automated logging and self-defending networks, informed recovery approaches, and agency-wide guidance for incident response. More agency-to-agency coordination will be required by the FY2008 timeframe. Specific initiatives that will be performed to carry out this strategy are provided below:

FY06

- **Develop Strategies and Policies for Points of Egress and Ingress**
  Develop an enterprise-wide strategy and associated policies for implementing security services for ports of egress and ingress, including FAA telecommunication infrastructure, public web servers, and internet access points.

- **Increase Enterprise-Wide Cyber Security Presence**
  Achieve a 20 percent increase in enterprise-wide cyber security presence through developing business agreements with TSIRC and NAS (Security Information Group).

- **Develop Strategy and Other Required Documents for IPv6 Security**
  Support ARD-1 in the development of a strategy for the transition of FAA business and administrative networks to the next generation of Internet Protocol Version 6 (IPv6). Identify and document a baseline of IPv4 security controls. Migrate baseline security controls into IPv6 and analyze IPv6 capabilities for potential security enhancements.

- **Implement Security Information Management (SIM)**

Implement a Security Information Management (SIM) solution that will provide the FAA CSIRC greater situational awareness capability through near real time processing of information systems security alerts.

- **Cyber Security/IT Research and Development**
  Establish partnerships with at least three other government agencies or academia; leverage (at least $20 million) their cyber security/IT research and development investments for the benefit of the FAA

FY07 – FY08

- **Continue FY06 Thrusts**

- **Investment in Informed Recovery and System Monitoring**
  Advance understanding and use of appropriate situational awareness approaches and tools through careful investments and internal projects to discover cost effective systemic monitoring techniques, such as automated logging and self-defending networks and agency-wide guidance for incident response. More agency-to-agency coordination will be required by the FY2008 timeframe.

Cyber Security: Begin a Phased Integration of Logical Access Controls into FAA Processes through DOT CIS Identity Credentials

This strategy supports the second set of outcomes by helping to build a major new capability for electronic authentication (e-authentication) and logical access control requirements of Federal Information Processing Standard (FIPS) 201 requirements. This will ensure a cyber security leadership position and ensure we can operate securely in the future. In FY2006, the strategic initiative will be to coordinate logical access control planning for alignment with DOT's Common Identification Standard (CIS) for its implementation. FY2007 – FY2008 initiatives will begin the migration to a common identity management system that complies with FIPS 201 and DOT requirements. The initiatives for this strategy follow:

FY06

- **Phased DOT Homeland Security Presidential Directive (HSPD) -12 Logical Access Control Integration**
  Develop the FAA ISS required documentation to comply with the authentication and logical access control requirements of FIPS 201 in support of the FAA HSPD-12 effort. Align the FAA logical access control planning with DOT's Command Identification Standard for the implementation of personal identity verification policy for a common identification standard for all Federal employees and contractors.

FY07 – FY08

- **Continue FY06 thrusts**

- **Migration to a Common Identity Management System that Complies with FIPS 201 and DOT Requirements**

Table: Summary of Corporate Information Technology Strategies and Initiatives

The table that follows summarizes the corporate IT strategies and initiatives for FY2005 – FY2008, and will be used to track the status of the two sets of outcomes. For each outcome the individual initiatives that will be carried out are listed, along with the organization or individual(s) responsible, timeframe for completion, and performance measures.

Table: Summary of Corporate Information Technology Strategies and Initiatives (1 of 7)

Outcome #1: Hold the gains we have achieved in cyber security, business value, and e-government.				
Initiatives		Who	Timeframe	Comments/Measures
1.A Business Value and Performance: Mature and Evolve OMB 300 Development and Review				
1.A.1	Exhibit 300s	AIO	FY06 – FY08	
1.A.2	Implement Earned Value Management (EVM)	AIO	NLT 4th quarter FY07	
1.A.3	Monitor EVM	AIO	FY07 – FY08	
1.A.4	Exhibit 53	AIO	FY06 – FY08	
1.B Business Value and Performance: Link OMB 300 Development and Review, Enterprise Architecture, and Program Execution				
1.B.1	Establish an Architectural Review Board (ARB) within the FAA acquisition process	AIO/JPDO/LOB & SO	FY06	
1.B.2	Monitor program compliance with the enterprise architecture and provide feedback into the CPIC and acquisition process	AIO/JPDO	FY07 – FY08	
1.B.3	Enhance the existing FAA configuration management process	AIO/JPDO	FY07 – FY08	

Table: Summary of Corporate Information Technology Strategies and Initiatives (2 of 7)

Outcome #1: Hold the gains we have achieved in cyber security, business value, and e-government.				
Initiatives		**Who**	**Timeframe**	**Comments/Measures**
1.C Cyber Security: Evolve and Mature Essential Elements of the FAA ISS Program in Order to Maintain an "A" Grade in FISMA				
1.C.1	Ensure all operational systems complete C&A or self-assessment	Owner: AIS-300 Prime Support: LOB/SO ISSMs	4Q06	
1.C.2	Remediate high vulnerabilities (DISP)	Owner: AIS-300 Prime Support: LOB/SO ISSMs	4Q06	
1.C.3	Ensure one-third of system inventory completes recertification	Owner: AIS-300 Prime Support: LOB/SO ISSMs	4Q06	
1.C.4	Achieve a "4" or better on the security portion of al exhibit 300s	Owner: AIS-200 Prime Support: LOB/SO ISSMs, AIS-500, AIO-20	FY06 – FY08	
1.C.5	Develop, document, and exercise an ISS Compliance Program	Owner: AIS-200 Prime Support: LOB/SO ISSMs, AIS-500	4Q06	

Table: Summary of Corporate Information Technology Strategies and Initiatives (3 of 7)

Outcome #1: Hold the gains we have achieved in cyber security, business value, and e-government.				
Initiatives		**Who**	**Timeframe**	**Comments/Measures**
1.C Cyber Security: Evolve and Mature Essential Elements of the FAA ISS Program in Order to Maintain an “A” Grade in FISMA				
1.C.5	Provide ISS awareness and specialized training	Owner: AIS-200	4Q06	
1.C.7	Develop baseline information security requirements	Owner: AIS-500 Prime Support: ARD/LOB/SO ISSMs	4Q06	
1.C.8	Develop a NIST compliant C&A process	Owner: AIS-300 Prime Support: AIS-500, LOB/SO ISSMs	2Q06	
1.C.9	Achieve 0.10 or fewer high vulnerabilities (SANS top 20)	Owner: LOB/SO ISSMs Prime Support: AIS-400	FY06 – FY08	
1.C.10	Establish Memorandum of Cooperation on Cyber Security in Concert with FAA’s AIA International Plans	Owner: AIS-500 Prime Support: AIA	4Q06	
1.C.11	Ensure mandated ISS program assessment and control capabilities	Owner: LOB/SO ISSMs Prime Support: AIS-300, AIS-200	FY07 – FY08	

Table: Summary of Corporate Information Technology Strategies and Initiatives (4 of 7)

Outcome #1: Hold the gains we have achieved in cyber security, business value, and e-government.				
	Initiatives	**Who**	**Timeframe**	**Comments/Measures**
1.D E-government: Maintain “Green” on E-Government Initiatives in the President’s Management Agenda Scorecard				
1.D.1	Maintain quarterly rating of green	AIO	FY06 – FY08	
1.D.2	Work with DOT to comply with deadlines for Presidential Initiative: Enhanced Human Resources Integration	AHR	FY06 – FY08	
1.D.3	Work with DOT to comply with deadlines for Presidential Initiative: Internet Protocol Version 6	TBD	FY06 – FY08	

Table: Summary of Corporate Information Technology Strategies and Initiatives (5 of 7)

Outcome #2: Achieve a leadership position in critical areas of IT including business value, IT performance and cyber security while controlling costs, standardizing and consolidating where appropriate, and building the capabilities to operate effectively and securely in the future.

Initiatives		Who	Timeframe	Comments/Measures
2.A Business Value and Performance: IT Optimization and Performance				
2.A.1	Semi-Annual Review of Corporate IT Performance			
2.A.1.1	Develop and confirm list of IT performance metrics	AIO, LOB/SO CIOs & IRMs	3rd Quarter FY06	
2.A.1.2	Perform semi-annual reviews of performance against metrics	AIO, LOB/SO CIOs & IRMs	4th Quarter FY06 – FY08	
2.A.2	Semi-Annual Review of IT Inventory			
2.A.2.1	Development of IT Inventory	AIO, LOB/SO CIOs & IRMs	2nd Quarter FY06	
2.A.2.2	Maintain IT Inventory and Perform semi-annual reviews of IT inventory	AIO, LOB/SO CIOs & IRMs	2nd Quarter FY06 – FY08	
2.A.3	Implementation of Optimized IT Inventory			
2.A.3.1	Server Consolidation	CIO Council	FY06	
2.A.3.2	Active Directory Consolidation	CIO Council	1st Quarter FY06	
2.A.3.3	Help Desk Consolidation	CIO Council	1st Quarter FY06	
2.A.2.4	ELAs, BPAs, etc.	AIO	FY06 – FY08	
2.A.2.5	Targeted single-reduced sign-on	AIO, LOB/SO CIOs & IRMs	FY06 – FY08	
2.A.3	Standards and Compliance	AIO	FY06 – FY08	
2.A.4	Workforce Training and Development	Owner: AHR LOB/SO support	FY05 – FY08	
2.A.5	Semi-Annual Reporting to ITEB	AIO	FY07 – FY08	

Table: Summary of Corporate Information Technology Strategies and Initiatives (6 of 7)

Outcome #2: Achieve a leadership position in critical areas of IT including business value, IT performance and cyber security while controlling costs, standardizing and consolidating where appropriate, and building the capabilities to operate effectively and securely in the future.				
Initiatives		Who	Timeframe	Comments/Measures
2.B Cyber Security: Develop Total FAA Cyber Situational Awareness in order to Enable the Right Hand Side of the Android Model				
2.B.1	Develop strategies and policies for points of egress and ingress	Owner: AIS-500	4Q06	
2.B.2	Increase enterprise-wide cyber security presence	Owner: AIS-400 Prime Support: LOB/SO ISSMs	4Q06	
2.B.3	Develop strategy and other required documents for IOv6 security	Owner: ARD-1 Prime Support: ATO-A, ATO-O, AIO-1, FTI, AIS-500	4Q06	
2.B.4	Implement Security Information Management (SIM)	Owner: AIS-400 Prime Support: LOB/SO ISSMs/AIS-200	4Q06	

Table: Summary of Corporate Information Technology Strategies and Initiatives (7 of 7)

Outcome #2: Achieve a leadership position in critical areas of IT including business value, IT performance and cyber security while controlling costs, standardizing and consolidating where appropriate, and building the capabilities to operate effectively and securely in the future.				
	Initiatives	Who	Timeframe	Comments/Measures
2.B Cyber Security: Develop Total FAA Cyber Situational Awareness in order to Enable the Right Hand Side of the Android Model				
2.B.5	Cyber security/IT research and development	Owner: ARD-1 Prime Support: AIO-1	4Q06	
2.B.6	Investment in informed recovery and system monitoring	TBD	FY07 – FY08	
2.C Cyber Security: Begin a Phased Integration of Logical Access Controls into FAA Processes through DOT CIS Identity Credentials				
2.C.1	Phased DOT HSPD-12 logical access control integration	Owner: AIS-500 Prime Support: LOB/SO ISSMs, ARC	4Q06	

VI. IT Initiatives for FAA Lines of Business and Major Staff Offices

In the previous section, we provided the corporate IT vision, outcomes, strategies, and initiatives for FY2006 – FY2008. Based on this information, the Lines of Business and major Staff Offices have identified ways that they are planning to contribute. This section documents their individual plans.

Airports (ARP)

The Office of the Associate Administrator for Airports (ARP) has the primary function of developing and implementing improved tools and processes, including airport engineering, safety and operations, hazard identification, training and risk management, airport compliance, airport planning and programming, airport safety and certification, safety data, financial assistance, national planning, passenger facility charge, and community & environmental needs. Our aim is to supply premium customer service both inside and outside the agency, to help improve aviation safety. Our organization also functions as a coordinator of military airport programs and safety related issues.

ARP's Information Technology (IT) systems will provide the highest quality service by designing its architecture and support to meet current and future needs. The IT infrastructure will ultimately allow ARP to increase efficiency and improve customer service. To achieve this aim, ARP will meet certain goals and objectives over the next six years. Those goals include allowing cross regional data access for all the Airports regional offices and enhancing Information Technology security measures.

An implementation strategy is key to a successful Information Technology Strategic Plan. At the core of this plan are the people, the processes, and the technology. These three pieces are interdependent on each other. Many other factors come into play in this strategic plan, funding, management feedback, responsiveness, a plan for infrastructure improvement, and input from regional offices.

ARP plans to pursue the following IT and ISS initiatives in FY06 through FY09.

- Provide capability for Airport sponsors to access and enter information into the Passenger Facility Charge (PFC) Information System.
- Auditing process and capability
- Account Management Process
- Initiatives to support HSPD12
- Initiatives to support transition to IP Version 6.
- On Demand Software Self Installation of approved applications

- Continue Reducing the number of usernames and passwords (Single-Sign On)
- Server standardization
- Improve IT procurement process to reduce cost
- Conduct service consolidation to reduce the required protocols and ports required by the ARP infrastructure
- Partner w/ FAA CSIRC for SCAP and scanning initiatives
- Perform remediation on issues identified in the SCAP and 800-26s.

ARP will also continue to initiate system improvements and refinements based upon user suggestions and business process needs.

Air Traffic Organization (ATO)

ATO Director of IT Operating Plan 2006 – 2008

Products and Services

Customers

The IT Directorate primary customer base encompasses all ATO Federal and contractor personnel resident within any FAA facility under the control of the ATO. Additionally, it includes all ATO contractor personnel not resident in ATO controlled facilities, having a business need to access ATO information systems to perform their assigned tasks. This directorate must provide the IT services to satisfy the business needs of the ATO workforce. All information services must available to and for ATO employees on a 24/7 basis, independent of their physical location or position within the ATO. In simple terms, all ATO employees must be able to access and manage their information assets from their workplace, their temporary duty station, or from their home to maximize the responsiveness of the ATO to meet real-time business demands. Secondary customers of the ATO IT Directorate will be the American public though the consistent distribution of reliable and validated sources of information related to the ATO.

Products and Services

FY-06 Products and Services

Implementation of standardized Mission Support and Administrative local area networks/wide area network
Implementation of Identity Management architecture
Implementation of first third of IT standardized desktops/platforms
Continued development and implementation of standardized ATO MIS/EIS fully web enabled applications
Establishment of regional call centers
Base lined cost of ATO-wide non-NAS IT services
Development of service level agreements within ATO

FY-07 Products and Services

Second third of IT standardized desktop implementation.
Enterprise-level server/server farm implemented for the ATO
100% implementation of remote maintenance capability by end of FY08
100% implementation of identity management

FY-08 Products and Services

Last third of IT standardized desktop implementation

Service Initiatives and Priorities

How we will align with FAA Flight Plan initiatives, improve our workforce, manage costs, and improve our processes?

Organizational Excellence

The IT Directorate directly contributes to the ATO Organizational Excellence goal by improving the quality, timeliness, and distribution of business information to enable data driven decision making within the ATO. The standardization of services, means and methodologies is anticipated to increase IT services reliability, and security. Additionally it is the intent of the IT Directorate to lower the cost of providing these services, and in doing so, free up human capital to support the ATO core business, that being separation assurance (safety) and flow management.

Improve Workforce

The standardization of IT services and products throughout the ATO will permit a higher level of training for the standardized toolsets to be used within the ATO. By reducing the variability in the means and methods and the data sources, more fiscal resources should be available to improve the skills of the workforce toward better decision making processes and in turn contribute to improved general service levels throughout the ATO customer base. Employees will be able to work anywhere within the ATO without requiring additional training on the administrative tools and process used to perform their work. This will provide greater employee mobility, increased management flexibility and lower operating cost.

Manage Costs

As there is limited information to baseline for the cost of IT goods and services, this is one of the greatest areas for improvement. It is documented throughout the IT industry, that a well run, centralized, standardized IT services provider will deliver an optimum suite of services at a much lower price than a dozen or more service providers providing a disparate set of services. We anticipate a theoretical cost reduction of at least 20% from baseline costs once they are established with any degree of certainty. Management of costs for IT services can be done once all IT budgets are centrally managed and services standardized throughout the ATO.

Improve Processes

The IT Directorate will contribute to this goal through the standardization of information delivery and through improving the quality of data sources used to make business decisions throughout the ATO. Additionally, it is a goal of this directorate to increase the transparency of decision making by improving communications throughout the ATO. Reliable and readily accessible data sources will directly contribute to the improvement of ATO business process.

Improve Processes

The IT Directorate will contribute to this goal through the standardization of information delivery and through improving the quality of data sources used to make business decisions throughout the ATO. Additionally, it is a goal of this directorate to increase the transparency of decision making by improving communications throughout the ATO. Reliable and readily accessible data sources will directly contribute to the improvement of ATO business process.

Service Delivery Commitments and Performance Metrics

Our major accomplishments over the next 3 years!

Organizational Excellence, Improve ATO Workforce, Manage Cost, Process Improvement

Service Delivery

Service delivery will be base lined and negotiated across the ATO through a service level agreement (SLA) with the Service Unit VPs. It is envisioned that one SLA will be established between the Vice President for Acquisition and Business Services and the members of the Executive Council covering the core delivery and minimum service expectations between the IT Directorate and all ATO Service Units. Unique Service Unit needs outside the core SLA, will be negotiated in separate addendums to the core SLA. The core SLA will be based upon industry service levels. Service Unit Addendums will only address the unique business needs of the individual Service Unit that represent an increased service level need. Increased costs associated with the delivery of the additional services will be identified and borne by the service unit as a direct cost of doing business.

Performance Metrics

Performance will be measured using established industry-recognized standards.

Cost Per Seat

Unit costs will be established for the total cost of ownership and service delivery. The total cost will include the cost of the desktop computer, the cost of all commercial and in-house developed applications, training, network, remote access charges, and help desk/service and repair costs for mission support and administrative IT products and services. These costs will be applied to every user of the ATO network, Federal or contractor, and will no longer be assumed as a free service. The cost per seat will be baselined in FY-06 using the best financial accounting that can be made with existing FAA accounting tools. These costs, once established, will be compared against comparable IT intensive Federal and commercial entities with a target goal not to exceed 95% of the industry average cost per seat.

Customer Satisfaction

Standardized customer satisfaction data will be collected across the ATO IT services community immediately after they receive services from the IT Directorate. A target goal of 85% customer satisfaction is the desired target customer satisfaction level. We anticipate that during the transformation to a standardized desktop and IT services suite, there will be a dramatic drop in initial customer satisfaction. Customer satisfaction ratings will be assessed and reported on a monthly interval. Customer satisfaction cannot be used as a stand-alone metric and must be balanced with the other service metrics.

Service Response Time

Service response time will be collected for the different support categories negotiated in the SLA and the respective addendums. These response times will be reported on a regular basis. The target for this goal will be that this directorate meets or exceeds the negotiated service response time 95% of the time.

Service Availability

As IT services are integral to the delivery of all ATO services, a target service availability level will be established within the core SLA. This negotiated availability will establish a reasonable desired availability rate for all IT services within the ATO; even under denial of service attacks and other IT security and vulnerability threat conditions. A baseline for this metric has not been established nor is one foreseen until a standardized level of service, network design and other standardization efforts are completed. The variability of architectures, desktop configurations, software applications greatly affect this metric at this time. It is anticipated that this metric can be baselined in at the end of FY07 when two thirds of the ATO has been standardized.

Challenges and Issues
What could impede our ability to achieve our commitments?

The key challenge in this endeavor will be the transformation from a fully decentralized, non-standardized IT environment to a centralized, and standardized, web-services based environment. At the heart of this issue will be the cultural aspects associated with the perceived loss of control. Clear and consistent communication with the leadership in ATO should provide the support necessary to proceed with the initial phases of changing the IT program. As successful centralized products and services come on line, it is anticipated that the business units and systems owners will realize the benefit of corporate data services. In reality, the goal of this endeavor will be to permit the user base to concentrate on their organization's content and business processes while reducing the cost of delivering the content to the ATO.

Aviation Policy, Planning and Environment (AEP)

The Office of Aviation Policy Planning, and Environment (AEP) provides critical support to the Administrator and FAA organizations in two major program areas: (1) planning and policy development, and (2) environment and energy programs. AEP accomplishes its goals by being the agency's focal point for strategic plan development and coordination; by identifying policy issues, and by developing, recommending and coordinating national aviation policy related to FAA authority; national airport and airway system development, operation, and finance; and environmental and energy matters. It is responsible for forecasting aviation activity to be incorporated in FAA plans and evaluating proposed and final FAA rules to assure that there is reasonable likelihood that anticipated benefits of rulemaking exceed costs. The office also supports the Management Advisory Council (MAC) in its statutory oversight of the FAA in general and the emerging performance based Air Traffic Organization in particular. It is responsible for developing national aviation policy related to environmental and energy matters. The office represents the United States in development of international standards related to aviation noise and engine emissions in international forums. The office is also responsible for providing policy guidance and technical assistance for FAA compliance with applicable environmental, occupational safety and health and energy statutes and regulations prescribing Federal environmental protection, worker protection, and energy conservation policies.

To ensure the above, AEP's policy and economic analysis programs support safety and capacity-enhancing initiatives of the agency, provides superior decision support tools and helps develop responsive strategies that allow aviation to grow in an environmentally responsible manner. Activities under the FAA's goal of Organizational Excellence revolve around supporting agency initiatives to help employees see the link between their jobs and agency goals.

Information Technology supports all of the above activities. In particular AEP maintains an extensive environmental modeling program, and a Business Planning and Tracking toolkit. Because of its need to respond immediately to policy and staff requests a very responsive "help desk" facility is also maintained.

In the past few years AEP has created a state of the art modeling facility supported by in-house staff. AEP has responded to the cost control initiative of the Flight Plan by streamlining its IT support and product set, while still continuing to keep its IT infrastructure robust. In the past two years, AEP has:

- Consolidated the IT operations of AEE, APO, and AEP to a single staff.
- Eliminated its contractor IT support.
- Reduced permanent FTE support staff by 25%.
- Reduced the numbers of operating servers by 55%.
- Reduced annual operating costs through consolidation and standardization of equipment and programs.

- Improved help desk response time.

In FY06-08 AEP will continue to maintain its high level of modeling and business planning tools, seeking to integrate these with other agency and industry tools that are consistent with its requirements. Similarly AEP will, to the extent practicable, support agency wide initiatives such as consolidation and cost control, while seeking to ensure that its need for highly responsive staff and policy work, and its robust strategic planning and modeling support, are not compromised.

Aviation Safety (AVS)

AVS Information Technology Strategic Goals FY 2006 - 2010

Goal 1: Expand the Application of Common IT to Enhance AVS Workforce Efficiency and Effectiveness

Strategies:

- National Applications: continue consolidation of AVS applications based on "services" (surveillance, designee management, certification, continued operational safety, etc.)
- AVS Data Center: operational applications in CAMI and the Registry will move to the data center (all others are completed)
- Servers: Consolidation of hardware in AVS geographic locations that house multiple AVS organizations (regions, some field offices)
- AVS National Help Desk: All users will call one help desk for 24 x 7 support
- FTE IT support in the field. Redefine FTE roles to align to changes in the IT environment. Train computer specialists in IT fields that will support the AVS business (applications, data analysis, collaboration, etc.).

Goal 2: Improve Alignment of IT Priorities based on AVS Priorities

Strategies:

- Allocate IT resources (money and people) based on AVS strategic goals.
- Develop an AVS IT governance policy that is in alignment with AVS goals.
- Expand the use of the Enterprise Architecture to support business decisions.

Goal 3: Improve Data Accessibility and Data Sharing

Strategies:

- Through the use of the Enterprise Architecture, NASDAC and other tools, make data (from multiple sources) more easily accessible to management and employees.

Goal 4: Invest in our IT Human Capital

Strategies:

- Provide opportunities for AVS IT resources to obtain certification in IT fields. Emphasize training and certification in areas that will be prominent in the future (enterprise architecture, program management, investment analysis, earned value management).

- Redefine FTE roles to align to changes in the IT environment. Train computer specialists in IT fields that will support the AVS business (applications, data analysis, collaboration, etc.).

Goal 5: Improve IT Support and Services to the AVS Workforce

Strategies:

- Offer new technologies that increase collaboration, data sharing and support business goals
- Offer 24 x 7 IT support to the workforce and external users
- Define methods for measuring IT support and services provided to AVS employees

Communications (AOC)

The Office of Communications (AOC) is responsible for the development, executive direction, and overall management of effective internal and national Communications programs. The office initiates and participates in the execution of coordinated plans and programs to make sure that major programs, policies, objectives and achievements of the FAA are effectively presented to FAA employees, the public and the aviation community.

A key aspect of FAA communications today is an effective web management program, for which AOC takes full responsibility. This includes providing standards, procedures and other requirements for the FAA web that all FAA organizations must follow. To help carry out these responsibilities, AOC has an agreement with AIO and ATO to host, operate and maintain the web server infrastructure for the FAA websites for the public, http://www.faa.gov and for employees, http://employees.faa.gov. In addition, ATO is leading the agency's cost control initiative to consolidate web servers at the William J. Hughes Technical Center.

The **web IT vision**: A robust, secure, efficient and reliable web infrastructure that makes the FAA web available to the public and employees at all times, from anywhere.

To achieve this vision, the goals and outcomes for FY2006-2009 are:

1. **Goal**: Improve the performance and reliability of the FAA web infrastructure and network.
   Outcome: FAA web page response for the user is within 6 seconds and achieves 99% availability.
   a. **Initiative**: Work with AIO and ATO to define requirements for and enhance the existing web server infrastructure.
   b. **Initiative**: Explore options and benefits for moving to a private sector provider to host, operate and maintain the FAA web servers.

2. **Goal**: Provide full backup capabilities for the FAA web to ensure the continuity of web operations in the event of a failure at the primary facility.
   Outcome: A full back up and recovery facility for the FAA web is in place, tested and ready to implement within 4 hours of a failure at the primary facility.
   a. **Initiative**: AIO and ATO work with the backup facility to provide a full-mirrored FAA web and web operations and maintenance services.

3. **Goal**: Limit access to the employee website on the Internet to FAA employees.
   Outcome: Only FAA employees can access information and tools on the employee website on the Internet.

a. **Initiative:** Determine and implement an effective and cost efficient solution to restrict access to the employee web that does not deter employees from using it.

b. **Initiative:** Make it easy to get to agency intranets through the secure, access controlled employee website.

4. **Goal:** Consolidate web servers for static content at a single facility
Outcome: A centralized, reliable, cost efficient web hosting operation.
   a. **Initiative:** Accelerate the migration of web servers and static web content to the Technical Center.

Financial Services (ABA)

In FY03 FAA converted from the old Departmental Financial Accounting System (DAFIS) to the new Department Financial Management System (Delphi). Responsibility for the operation, integration and enhancement of the FAA Procurement System (PRISM) was also transferred to the Office of Financial Services.

Our primary focus in FY2006 is to provide additional functionality to both Delphi and Prism to support financial management and procurement activities. We plan to integrate and consolidate legacy feeder and financial reporting systems working closely with the LOB's. In doing this we will implement an integrated Configuration Management (CM) program across all agency and departmental financial management systems. ABA will lead agency wide financial management system planning based on industry best practices in full systems life cycle management.

In addition to managing the implementation of these DOT core financial systems ABA has developed and is implementing an FAA wide Cost Accounting System to report the full costs of producing intermediate and end user services. In FY2006 ABA will complete the full implementation of CAS within FAA.

Since our primary focus will be on the financial system operation, enhancement, and operations, ABA will be looking to reduce our need to procure and maintain an independent IT infrastructure for ABA. In FY06 we will develop a plan to outsource our office automation support and transition in FY07 once a suitable service provider is found. In addition, we plan to begin the process of transferring our existing applications and their associated IT hardware to one of the approved FAA Data Center's in an effort to reduce costs.

Human Resources Management (AHR)

People are the foundation for FAA's mission accomplishment. The Office of Human Resource Management (AHR) advises on and supports the management of FAA's people. Only a skilled, knowledgeable, diverse, and high-performing workforce can handle the demands of achieving FAA's safety, capacity, and international aviation goals. AHR's intention is to support these goals by creating innovative, flexible, and efficient personnel systems and policies. Some specific examples of strategic initiatives currently under way and planned are outlined below:

SWIFT

The Office of Human Resources plans to Expand the HR Selections within Faster Time (SWIFT) automated suite to all mission-critical positions and those positions that cross organizational lines, i.e., finance, budget, human resources, and information technology. The enhanced modules will support the recruitment and placement process, for both external and internal positions. The advanced Automated Staffing and Application module under the SWIFT program will include tracking of security clearance/waiver and medical exams.

Develop interface to integrate recruitment (vacancy announcement) information to USA jobs, in support of the e-Government Initiative, "Recruitment One Stop." This activity included the completion of the developments necessary to interface and integrate recruitment information (vacancy announcement) into the USAJobs database.

Federal Personnel and Payroll System

Implement the Federal Personnel and Payroll System (FPPS), the Electronic Learning Management System (eLMS), and other supporting Subsystems within FAA in accordance with established timelines.

FAA will complete the migration to the FPPS in FY 06. There will be an ongoing effort to enhance the system to meet our many diverse pay and personnel rules in order to make them more efficient and at the same time allowing for innovation and flexibility. AHR will monitor and manage the implementation of all necessary system changes that are proposed over the next several years to ensure that the system remains innovative, efficient, and flexible.

AHR will also manage the migration of the learning and management automated processing from FAA legacy systems to the new E-Learning Management System (e-LMS). Piloting of the Competency Management Functionality in AHR is expected the first quarter of FY 06. AHR will be monitoring and managing the implementation of all system change requests, after initial deployment, to ensure that the system remains up to date

AHR will also be supporting the migration of the time collection and labor reporting automated processing from DOT legacy systems to CASTLE.

The Enterprise Human Resource Integration Initiative

AHR, in conjunction with the Department of Transportation (DOT), has initiated an effort to implement the Electronic Official Personnel Folder (E-OPF). Once completed DOT and FAA employees will have access to a consolidated data view of their personnel folder that documents their employment actions and history. AHR staff will process automated transactions that become a part of the E-OPF and the data will become a part of a digital file that will eliminate the need to maintain and keep paper records. The current plans are to migrate the AHR Western Service Center's existing Documetrix system to meet the OPM EHRI standards in FY 06. The two remaining AHR Service Centers will be converted and brought on line sometimes during FY 07.

Develop enterprise-wide HR information systems

AHR will continue to work toward eliminating duplicate systems and applications and replacing them with enterprise-wide HR information systems. AHR is currently working with the Assistant Administrator for Regions and Centers (ARC) to review and evaluate all ARC maintained systems in regions against FPPS functionality to ensure that there is not duplication. This is an ongoing effort that will continue throughout FY 06 and beyond. The review will also target systems that have the same or nearly identical functionality to see if they should be consolidated into enterprise-wide HR information systems.

International Aviation (API)

API is a staff office responsible for FAA's international aviation policy. We provide liaison and coordination with the U.S. foreign affairs community and international organizations, manage international technical assistance activities and agreements for cooperative activities, and provide guidance and support for FAA personnel stationed overseas and for those on TDY assignments.

IT allows us to be in closer communication with the external international community and with those inside the FAA engaged in international activities. Our primary goals are to collaborate and coordinate policies and activities, to rapidly gather and disseminate information, and to do so in a securest manner practical.

Environment

API employs about 100 people including contractors at 11 locations. All but 2 of the locations are overseas.

- API Regional offices are located in Brussels, Miami, and Singapore
- FAA Senior Representatives' Offices are either co-located or at American Embassies:
  - Abu Dubai, London, Moscow, and Paris (reporting to Brussels
  - Beijing and Tokyo (reporting to Singapore)
  - Dakar and US Mission to ICAO in Montreal (reporting to Washington)
- FAA Brussels is the only field location where API maintains a LAN. The other regional offices share a network hosted by other LOB's.
- FAA Senior Representatives reach FAA's network through FTI remote access.
- API at Headquarters has an SLA with ATO to provide LAN support, software, and other services.

U.S. Government and FAA policies are driving greater consolidation of IT services.

API IT Goals by FY 2008

- Continuous business process improvement implemented
- IT services consolidated
- IT security and disaster recovery plans implemented, reviewed and practiced.

Strategy

- Plan and implement improved IT security and disaster recovery procedures in first-half of FY06
- Use the information gathered in preparing and implementing security and disaster recovery plans:
  - To prepare a business case for IT consolidation of API field locations with options for using other LOBs, contractors, or creating API IT FTE's
  - To centralize API IT support in FY07 to the extent that there is a business case and resources for doing so.
- Develop process to improve the effectiveness and efficiency of API business processes using standard FAA IT systems and applications. (FY-06)
- Implement continuous Business process improvements (FY-06-07-08) including
  - Collaboration with State Department and organizations in the foreign affairs community
  - Collaboration with other FAA organizations for improvement of agency wide international processes.

Regions and Center Operations (ARC)

ARC's IT mission is to provide Desktop Support, E-Mail, Help Desk Support, Information Systems Security, Infrastructure Support, Systems Applications Development, and Enterprise Information Technology Acquisitions to serve ARC's internal and external customers across the nine Regions and the Aeronautical Center. A major goal in FY-06 is the development of an ARC Enterprise Architecture Plan and IT Investment Strategy to support this plan. The overall ARC IT Strategic Plan is to (1) expand enterprise services, (2) improve financial management, (3) continuously improve customer service, (4) enhance IT system security, and (5) effectively train and develop employees.

Enterprise Services

ARC is focused on developing an IT strategy designed to maximize interoperability across all IT platforms. As a first step in this plan, ARC plans to work in tandem with each region to develop a standard configuration for ARC's IT infrastructure. For governance, an IT council will be established, consisting of IT managers at each region and at headquarters. The council will ensure that IT investments are made within existing budget constraints and are aligned with the established architecture.

Financial Management

ARC plans to improve IT financial management by focusing on investment strategies that leverage ARC IT funds across the Enterprise. This will be accomplished through the elimination of redundant processes, allowing funds to be invested more wisely and lower cost. ARC supports the Agency's Cost Control Program through Helpdesk Consolidation, Server Consolidation, and Application Consolidation.

Customer Service

ARC is focused on delivering effective, cost-efficient IT services to its customers, measuring progress through customer satisfaction surveys, improved help desk response times, and fostering more successful problem resolution through process improvement. ARC's goal is to provide customers with standardized services, processes, procedures, and products across the Enterprise. To this end, ARC will continue centralizing help desk support, expanding the Meta-directory prototype for Reduced Sign-On (RSO)/Single Sign-On, and continuing the migration to active directory to meet customer needs.

IT System Security

ARC provides leadership and technical expertise to effectively manage the Information System Security program. Key goals during the next three fiscal years include: 1) Ensure that no cyber events occur that disable or significantly degrade FAA services. 2) Ensure that all operational/deployed systems on the inventory have current certification and authorization (C&A) and undergo a self-assessment if full C&A is not required. 3) Remediate high vulnerabilities as identified in the DOT portal (DISP) as of October 1, 2005.

Employee Development

In line with the objective of building a world-class IT workforce, ARC is in the process of adopting a competency-based approach as the foundation for the professional development of its IT workforce. ARC IT managers will use competency checklist forms to identify gaps in training and work up individual development plans to address the career development needs of each employee. This approach will enable ARC to make more efficient use of existing IT skills and reduce costs associated with unproductive training. Gaps will be addressed through greater use of computer-based leadership training, mentoring, job rotation, and hands-on training.

The Enterprise Services Center (ESC)

A key aspect of ARC's strategic thinking involves the implementation of process improvements. Process improvement is the underpinning of the objectives outlined above. As an example of ARC's movement toward continued process improvement, the Enterprise Services Center at the Mike Monroney Aeronautical Center stands as a major stronghold. As a government-wide Financial Management Center of Excellence (COE), the ESC provides accounting services and financial systems for the Department of Transportation (DOT), including the Federal Aviation Administration, and other agencies in Federal government. The ESC's strategy for the next three years complements the FAA Information Technology Strategy in Business Value and E-Government. By leveraging the existing technology investments, economies of scale are created that benefit not only the FAA but also the entire federal government and the taxpayer. Plans include the establishment of a more extensive configuration management program, establishment of a Project Management Office and Quality Office, and implementation of standard processes and infrastructure.

Conclusion

ARC is reviewing its current IT management processes and is committed to making them more effective and efficient through centralization and standardization to reduce duplication and decrease costs. ARC will be moving these plans forward into full implementation over the next three years, carefully measuring performance against strategic goals to improve effectiveness, efficiency, and fiscal responsibility.

Security and Hazardous Materials (ASH)

ASH has been working a high-level program for FY05. We will continue working on these projects in FY06-FY09. ASH has been designated the lead office for HSPD-12 and the Forensics Program. Currently all ASH 334's have be certified as Digital Computer Forensics Specialists. We have also made huge gains in Server Consolidation, Helpdesk Consolidation, and Cell Phone Consolidation.

Server Consolidation – HQ

Approximately two years ago, ASH began the task of server consolidation within HQ. ASH has successfully consolidated from 34 servers to 8 servers, whereby saving the Agency approximately 700k. We are now beginning to look at consolidating servers in our regional offices.

Helpdesk Consolidation

ASH has successfully consolidated our HQ's and regional helpdesk into one helpdesk located in HQ's. The helpdesk is the first line of support for all web-based and desktop issues for ASH employees. This helpdesk also handles all support pertaining to E-QIP (Electronic Questionnaires for Investigations Processing) for the Agency. ASH is also the third tier support for ARC in HQ's.

Cell Phone Consolidation

Two years ago, ASH began the task of consolidating cell phones. At the time, we were using approximately 550 cell phones at a cost of approximately 800k dollars. We have since brought our cell phone totals to 150 cell phones at a saving of approximately 500k a year.

For the next three years ASH will be focusing on:

- HSPD-12
- Forensics Program
- Server Consolidation

In FY06 ASH will be concentrating its efforts on HSPD-12. This is an extremely high profile project, which will eventually be adopted by the Department and become a department wide system. ASH is using every available resource to ensure the FAA succeeds in this endeavor.

ASH's strategic plan for the next three years is in the high range, in comparison to the FAA Strategy.

VII. Monitoring and Controlling the FAA IT Strategy

Monitoring and controlling the FAA IT strategy will ensure that potential problems can be identified in a timely manner and corrective action can be taken, when necessary. The key benefit is that strategy performance is observed and measured regularly to identify variances from the plan. Continuous monitoring provides insight into the health of the strategy and highlights any areas that require additional attention. Controlling changes and recommending preventive action in anticipation of possible problems ensures that the strategy proceeds on the right track.

In order to monitor and control the FAA IT strategy, it will be necessary to collect, measure, and disseminate performance information, and assess measures and trends to effect improvements. Risk monitoring is required as well, to ensure that risks are identified early, their status is reported, and appropriate risk plans are executed.

On a quarterly basis, AIO will review the status of the FAA IT Strategy, using the *Table: Summary of Corporate IT Initiatives* that was presented in Section V as the framework for reporting. The results of these reviews will be provided to the ITEB and will include the following outputs:

- ***Recommended Corrective Actions***
  Corrective actions are documented recommendations that bring expected future performance into conformance with the strategy.

- ***Recommended Preventive Actions***
  Preventive actions are documented recommendations that reduce the probability of negative consequences associated with risks.

- ***Forecasts***
  Forecasts include estimates or predictions of conditions and events in the future, based on information and knowledge available at the time of the forecast. Forecasts are updated and reissued based on work performance information provided as the strategy is executed.

- ***Requested Changes***

The ITEB will make decisions on the outputs listed above that are designed to get the strategy back on track or enable appropriate changes.

Federal Aviation
Administration

Appendix I: Source Documents

1 The President's Management Agenda (Summer 2001)

2 FAA Strategic Flight Plan 2005 – 2009

3 Information Services Fiscal Year 2005 Business Plan

4 Airports (ARP) Fiscal Year 2005 Business Plan

5 Air Traffic Organization (ATO) Fiscal Year 2005 Business Plan

6 Commercial Space Transportation (AST) Fiscal Year 2005 Business Plan

7 FAA IT Strategy, CIO Council (December 8, 2004)

8 FY06 Federal Enterprise Architecture (FEA) Reference Model Revisions (July 30, 2004)

9 FY06 Federal Enterprise Architecture Additional Instructions, OMB FEA Program Management Office (July 30, 2004)

10 FAA AIO/CIO Roles and Responsibilities, CIO Position Paper (Draft, January 13, 2005)

11 FAA Data Management Program presentation to the ITEB, September 8, 2005

12 Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004)

13 Federal Information Processing Standards Publication (FIPS PUB) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors (February 25, 2005)

14 ISS FY05 Strategic Plan

15 AIO/AIS Business Plans

16 FAA LOB/SO Business Plans and Organizational Charts

17 FAA IT Strategy, CIO Council (December 8, 2004)

18 FY06 Federal Enterprise Architecture (FEA) Reference Model Revisions (July 30, 2004)

19 FY06 Federal Enterprise Architecture Additional Instructions, OMB FEA Program Management Office (July 30, 2004)

20 FAA 2007 OST Budget Submission

21 FAA AIO/CIO Roles and Responsibilities, CIO Position Paper (Draft, January 13, 2005)

22 FAA Chief Information Officer Council Initiative #6, Establishing FAA Directory Services -- Program Charter (Draft, June 7, 2005)

23 FAA Notice N 1100.300, Office of Information Services Restructuring (5/12/05)

24 GAO-04-822 Information Technology: FAA has Many Investment Management Capabilities in Place, but More Oversight of Operational Systems is Needed

25 GAO-05-23 Air Traffic Control: FAA's Acquisition Management has Improved, but Policies and Oversight Need Strengthening to Help Ensure Results

26 OMB A-11 Sections 53 and 300

27 05-06 Performance Plan for FISMA

28 Charter - Information Technology Executive Board (April 9, 2004)

29 Charter – Chief Information Officer’s Council (November 2004)

30 A New Look at Cyber Defense by Dan Mehan, http://www.faa.gov/aio/common/documents/NSF-ANSIBrief.pdf (October 2003)

31 Department of Transportation Strategic Plan 2003-2008 (September 2003)

32 GAO-05-266 Federal Aviation Administration: Stronger Architecture Program Needed to Guide Systems Modernization Efforts

33 FAA Office of Information Services Human Capital Plan, FY2005 – FY2009 (Draft, April 2005)

34 FAA Policy 1375.1C, *Data Management*, dated June 20, 2001, http://www.faa.gov/aio/common/documents/1375_1C.doc.

35 FAA ARD-1 500 Day Plan, dated August 10, 2005.

36 Transition Planning for Internet Protocol Version 6 (IPv6) (OMB Memorandum for Chief Information Officers, August 2, 2005). http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

37 GAO-05-471 Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks (May 2005) http://www.gao.gov/new.items/d05471.pdf

37 FAA Flight Plan FY2006 – FY2010 (Draft 7/7/05)

38 FAA Information Systems Security Plan FY2006 – FY2008 (Draft August 2005)

39 GAO-05-207 High Risk Series, An Update, (January 2005) http://www.gao.gov/new.items/d05207.pdf

40 FAA Order 1370.XX, Wide Area Network Connectivity Security (Draft August 16, 2005)

41 FAA Order 1375.1D – Information / Data Management (Draft September 9, 2005)

42 FAA Data Governance Board Charter (Draft September 9, 2005)

43 FAA Data Management Presentation to CIO Council, August 4, 2005

Federal Aviation
Administration

Appendix II: Acronyms and Abbreviations

This appendix will provide an inventory of all acronyms and abbreviations used in the preceding sections.

ABA	Financial Services
AEP	Aviation Policy, Planning, and Environment
AHR	Human Resources Management
AIO	Assistant Administrator for Information Services and Chief Information Officer
AIS	Office of Information Systems Security
AMS	Acquisition Management System
ARC	Region and Center Operations
ARP	Airports
ASH	Security and Hazardous Materials
ATO	Air Traffic Organization
AVS	Aviation Safety
BPA	Blanket Purchase Agreement
CA	Certification Authority
C&A	Certification and Accreditation
CCB	Configuration Control Board
CIO	Chief Information Officer
CIS	Common Identification System
CM	Configuration Management
CPIC	Capital Planning and Investment Control
CSIRC	Computer Security Incident Response Center
DOD	Department of Defense
DOT	Department of Transportation
EHRI	Electronic Human Resources Initiative
EOPF	Electronic Official Personnel Folder
ELA	Enterprise License Agreement
ELMS	E-Learning Management System
EVM	Earned Value Management
FAA	Federal Aviation Administration
FAA-iCMM	FAA integrated Capability Maturity Model
F&E	Facilities and Equipment
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FPPS	Federal Personnel Payroll System
FTI	FAA Telecommunications Infrastructure
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GAO	Government Accountability Office
GPEA	Government Paperwork Elimination Act
HSPD	Homeland Security Presidential Directive
iCMM	Integrated Capability Maturity Model

ID/EA	Identity Management/E-Authentication
IEE	Internal Efficiency and Effectiveness
IG	Inspector General
IPv6	Internet Protocol Version 6
ISS	Information Systems Security
ISSM	Information Systems Security Manager
IT	Information Technology
ITEB	Information Technology Executive Board
JRC	Joint Resource Council
LAC	Logical Access Control
LOB	Line of Business
NAS	National Airspace System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OST	Office of the Secretary
PIV	Personal Identity Verification
PM	Program Manager
PMA	President’s Management Agenda
PMP	Program Management Plan
QA	Quality Assurance
SANS	(SysAdmin, Audit, Network, Security) Institute
SCAP	Security Certification and Authorization Package
SIM	Security Information Management
SO	Staff Office
WAN	Wide Area Network

Appendix III: Links between FAA Strategic Goals and FAA IT Goals

	Increased Safety	Greater Capacity	International Leadership	Organizational Excellence
Goal #1: Business Value and Performance FAA IT aligned with the business and delivers value, its performance is measured, its resources properly allocated and its risks mitigated.	▒	NA	NA	■
Goal #2: Cyber Security Maintain the FISMA grade, achieve zero cyber security events that significantly disable or degrade FAA service, and complete the Android model.	■	NA	■	■
Goal #3: E-Government “Green” on E-government initiatives in the President’s Management Agenda scorecard and support, as appropriate, in the other three areas.	▒	NA	▒	■

Legend:
Black – Directly supports goal
Grey – Indirectly supports goal